PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number: **WO 99/13391**
G06F	**A2**	(43) International Publication Date: 18 March 1999 (18.03.99)

(21) International Application Number: PCT/US98/18571

(22) International Filing Date: 4 September 1998 (04.09.98)

(30) Priority Data:

60/058,153	8 September 1997 (08.09.97)	US
60/065,033	10 November 1997 (10.11.97)	US

(71) Applicant: NEOMEDIA TECHNOLOGIES, INC. [US/US]; Suite 600, 2201 Second Street, Fort Myers, FL 33901 (US).

(72) Inventors: CHRISTIANSEN, Robert; 5412 Burchette Road, Tampa, FL 33647 (US). DURST, Robert, T., Jr.; 6111 Tidewater Island Circle, Fort Myers, FL 33908 (US). GREENE, Jonathan, D.; Suite 504, 2001 Jefferson Davis Highway, Arlington, VA 22203 (US). KEEPPER, Lester, H., Jr.; Suite 303, 2001 Midwest Road, Oak Brook, IL 60621 (US).

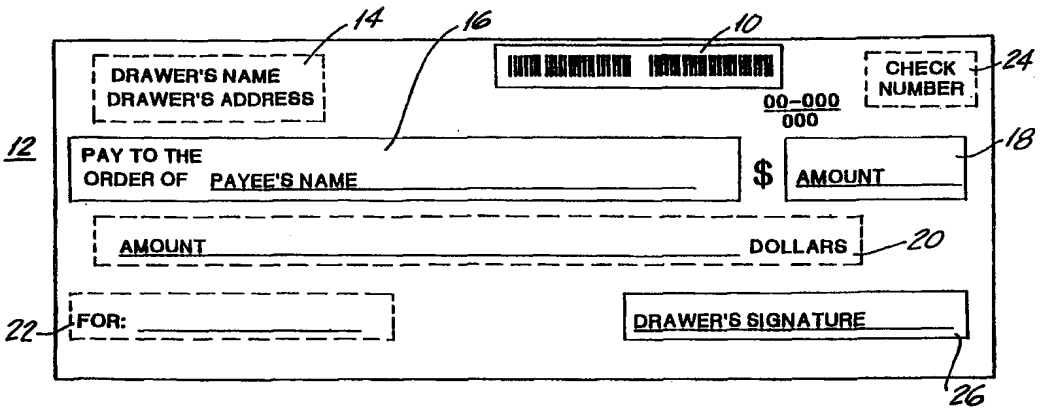
(74) Agent: BARKUME, Anthony, R.; Anthony R. Barkume, P.C., Suite 200, 14 South Main Street, Sayville, NY 11782 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: IMPROVED SECURE DOCUMENTS



(57) Abstract

A method of generating and verifying secure documents (12) wherein the secure document (12) is printed with machine–readable symbols (28) representing physical parameters of the secure document prior to application of hand or machine–printed indicia, human and/or machine–printed indicia appearing thereon, biometrics (finger and voice prints), and transaction history. In another embodiment, a two–stage imaging or watermark process captures an image of indicia within an area defined by a ultraviolet coating (30), prepares a bit map thereof and encodes the bit map and/or a derivative thereof in machine–readable symbols that are then printed on the secure document (12). Intrinsic verification of the secure document (12) is accomplished by comparing actual physical measurements and scannings of the secure document with the data content of the machine–readable symbols appearing on the secure document. Extrinsic verification of the secure document is accomplished by comparing information content resident in local and/or remote databases concerning the secure document or its transfer with the data content of the machine–readable symbols appearing on the secure document.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

IMPROVED SECURE DOCUMENTS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is based on and claims the priority of co-pending provisional patent application serial number 60/065,033 filed in the United States Patent and Trademark Office on November 10, 1997, and co-pending provisional patent application serial number 60/60,058,153 filed in the United States Patent and Trademark Office on September 8, 1997.

TECHNICAL FIELD

This invention relates to secure documents and in particular to the utilization of electromagnetic wave emission characteristics and machine-readable symbols in order to create secure documents.

BACKGROUND ART

The generation of fraudulent documents has increased greatly in recent years due in large part to the immense progress in printing and photocopying technology and its availability to individuals of all means. The average person will find no difficulty whatsoever in obtaining a color copying machine, color scanning machine, or a color laser printer for substantially less than what he would expect to pay for a reasonably well-equipped personal computer. Given such equipment, a user could scan the document, thereby obtaining a digital image which could then be manipulated using an appropriate program running on a personal computer. Such a program could then be used to make modifications in the digital image including, for instance, the amount to be paid and the payee of a check,

while retaining everything else including the signature of the drawer. The color laser printer would then be able to reproduce the image with such precision that the check would be processed by clearing houses and the drawer's bank without detection.

Prior art U.S. Pat. Nos. 4,588,211; 4,634,148; and 4,724,309, hereby incorporated by reference, teach the application of fluorescent material to specific areas of negotiable instruments in order to enable a machine to scan handwritten indicia applied over these areas such as signature, amount, payee, etc. U.S. Pat. No.4,157,784; hereby incorporated by reference, teaches the use of protective coatings, inks and paper over a printing ink having properties which will be disturbed and detectable if erasure is attempted. Another alternative which is disclosed in this patent is the addition of fluorescent properties to inner layers of the paper. If erasure is attempted the top coating or layer of the paper will be removed revealing the fluorescent properties of the inner layer which is immediately detectable under an ultraviolet light.

While the above methods tend to guard against the alteration of handwritten elements of negotiable instruments, it would be advantageous if in addition to or instead of these prior art methods the information in the negotiable instrument could be verified via machine-readable means in order to provide an extra level of protection against alteration or fraud which is relatively simple, efficient and cost effective. Such a method could also be applied to the verification of any document (e.g., deeds, wills, contracts, birth certificates, money orders, gift certificates, passports, labels, etc) or any other object

which would benefit from a secure means of ensuring authenticity.

The current system used for the processing of checks provides financial institutions with very definite time limits within which to determine whether or not to pay or dishonor a check. There is a growing demand for legislation which would provide financial institutions with a longer period to render this decision (float time). However, such legislation would only make matters worse for a check clearing process which is already considered by many to be archaic. Therefore, it would be advantageous if financial institutions were provided with additional time to decide whether to pay or dishonor a check while retaining or even shortening the overall duration of the check clearing process.

DISCOSURE OF THE INVENTION

In accordance with the present invention a method of generating and verifying secure documents such as checks, money orders, traveler's checks, passports, shipping labels, food stamps, and electronic fund transfers comprising machine-readable symbols is provided. In a first embodiment, the secure document is printed with machine-readable symbols representing physical parameters of the secure document prior to application of hand or machine-printed indicia. In a second embodiment, the secure document is printed with machine-readable symbols representing information not representative of physical parameters of the secure document prior to application of indicia such as human and/or machine-printed indicia appearing thereon, biometrics (finger and voice prints), and transaction history. In a third embodiment, a two-stage imaging or watermark process captures an image of indicia

within an area defined by a ultraviolet coating, prepares a bit map thereof and encodes the bit map and/or a derivative thereof in machine-readable symbols that are then printed on the secure document. Intrinsic verification of the secure document is accomplished by comparing actual physical measurements and scannings of the secure document with data content of the machine-readable symbols appearing on the secure document. Extrinsic verification of the secure document is accomplished by comparing information content resident in local and/or remote databases concerning the secure document or its transfer with data content of the machine-readable symbols appearing on the secure document.

In further accord with the present invention a fourth embodiment is provided which tracks the secure document in the form of a check using both intrinsic and extrinsic verification, which provides the advantage of increasing the amount of time in which the payor bank must make the decision to finalize payment on the check. A fifth embodiment provides a method for tracking the secure document in the form of a money order, which provides the advantage of intrinsic and extrinsic verification of authenticity by virtually every entity involved in the transfer of the money order. A sixth embodiment provides a method for tracking the secure document in the form of a food stamp, which provides the advantage of intrinsic and extrinsic verification of authenticity by virtually every entity involved in the transfer of the food stamp and, thus, removal of the need for government entities to maintain costly reserves in contemplation of fraudulent food stamps. A seventh embodiment provides a method for tracking a secure document which embodies an electronic fund transfer, which provides the advantage of intrinsic and extrinsic

verification of authenticity by virtually every entity involved in the transfer of the secure document.

Thus, the present invention encompasses a method of authenticating secure documents, comprising the steps of

manufacturing blank secure documents comprising secure portions, the secure portions comprising predetermined emission spectrum and characteristics upon exposure to electromagnetic radiation of a predetermined wavelength; applying handwritten and machine printed indicia to the blank secure document; scanning the secure document in order to obtain an image; developing a bit map or derivative thereof from the image; maintaining a database comprising the predetermined emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof and image as well as additional relevant information concerning the secure document and transactions involving the secure document; encrypting the predetermined emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof; compressing the encrypted predetermined emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof; encoding the compressed predetermined emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof into machine-readable symbols; printing the machine-readable symbols on the blank secure document; obtaining the emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof from the secure document; comparing the emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof with information contained in the machine-readable symbols upon decoding, decompressing and decrypting the machine-readable symbols, thereby enabling intrinsic verification of the secure document by

entities in a chain of circulation; and comparing the emission spectrum, characteristics, wavelength, indicia and bit map or derivative thereof and information contained in the machine-readable symbols upon decoding, decompressing and decrypting the machine-readable symbols with the database, thereby enabling extrinsic verification of the secure document by entities in the chain of circulation.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a negotiable instrument comprising an electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 2 illustrates an exploded view of the electromagnetic wave emissive machine-readable snippet of the present invention comprising a linear bar code.

Fig. 3 illustrates an exploded view of the electromagnetic wave emissive machine-readable snippet of the present invention comprising a two-dimensional bar code.

Fig. 4 illustrates a money order comprising the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 5 illustrates a passport comprising the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 6 illustrates a shipping label comprising the electromagnetic wave emissive machine-readable snippet of the present invention.

Figs. 7A and 7B are block diagrams illustrating a method for generating and verifying a secure document utilizing the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 8 is a block diagram illustrating a method for expediting information to financial institutions required in order to decide whether to pay or dishonor a check utilizing the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 9 is a block diagram illustrating a method for circulating a secure money equivalent utilizing the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 10 is a block diagram illustrating customer support services provided by a service bureau shown in Fig. 9.

Fig. 11 is a block diagram illustrating a method for distributing a secure food stamp utilizing the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 12 illustrates a negotiable instrument comprising an electromagnetic wave emissive machine-readable snippet of the present invention further comprising watermarks.

Figs. 13A-C is a flow chart illustrating a two-stage imaging or watermark process of the present invention.

Fig. 14 is a block diagram illustrating issuing and verification hardware packages to implement the two-stage imaging or watermark process of Figs. 13A-C.

Fig. 15 is a block diagram illustrating a recursive implementation of the two-stage imaging or watermark process of Figs. 13A-C.

Fig. 16 is a block diagram illustrating a method for distributing a secure suspended EFT utilizing the electromagnetic wave emissive machine-readable snippet of the present invention.

Fig. 17 is a flowchart illustrating a method for issuing secure money orders.

Fig. 18 is a flowchart illustrating a method for issuing secure gift certificates.

Fig. 19 illustrates a credit card and a money order comprising a travelling signature card embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Fig. 1 illustrates a negotiable instrument in the form of a check 12 comprising an electromagnetic wave emissive machine-readable snippet 10 of the present invention. The check 12 also comprises zones having information or indicia imprinted therein, typically found on all commonly issued checks such as a drawer's name and address zone 14; a payee's name zone 16; a numerical amount zone 18; an alphanumeric amount zone 20; a memo zone 22, a check number zone 24; and a drawer's signature zone 26. These zones may additionally utilize the techniques of the

prior art disclosed in U.S. Pat. Nos. 4,588,211; 4,634,148; 5,456,498; and 4,724,309; hereby incorporated by reference. Briefly, the aforementioned prior art patents disclose a method whereby a fluorescent coating is applied to one or more of these zones, and upon application of ultraviolet light to these zones, the indicia, handwritten or printed by machine on top of the fluorescent coating, is highlighted permitting it to be detected and scanned by machine or human operator.

Fig. 2 illustrates the electromagnetic wave emissive machine-readable snippet 10 of the present invention which comprises a machine-readable symbol, or in the case of Fig. 1, a linear bar code 28 within a coating or ultraviolet (UV) snippet 30 which exhibits predetermined luminescent, phosphorescent or fluorescent properties. The order of application of the machine-readable symbol 28 with respect to the coating 30 is not critical to the scope of the present invention. However, the order may be important during the scanning and detection steps depending upon the characteristics of the application processes. The preferred embodiment or most likely scenario is that the coating will be applied by, for instance, using a lithographic technique during the manufacture of the blank check 12 or stock and the machine-readable symbol 28 will be printed over the coating 12 at some point thereafter. The machine-readable symbol 28 is printed by the drawer prior to issuance of the check 12 and/or the check printing company prior to making the checks available to the drawer. Thereafter, an attempted alteration of the machine-readable symbol 28, such as by "shaving" off the machine-readable symbol 28 from the surface of the check 12, will likely either deface the coating 12 or render it non-uniform which becomes obvious upon inspection during verification by means well known in

the art. For instance, areas in which the coating 12 is removed will appear as darkened areas against the lighter background of the uniform coating under, for instance, ultraviolet light. In addition, making fraudulent alterations appear valid is made more difficult by the fact that only certain sequences within the machine-readable symbol 28 are accepted as valid as well as the utilization of additional authentication methods which may optionally be applied to the machine-readable symbol such as checksums, Cyclic Redundancy Check (CRC) sequences, parity sequences as well as other equivalent means well known in the art. These methods guard against alterations which involve adding or removing portions of the machine-readable symbol 28.

Fig. 3 illustrates substitution of a two-dimensional bar code 36 for the linear bar code 28 illustrated in Figs. 1 and 2. The two-dimensional bar code, such as the two-dimensional portable data file PDF 417, comprises multiple rows of codewords. Each codeword is a mark pattern comprising a plurality of elements or marks. The marks can be of various heights, as in a linear bar code, or can be of a relatively small height to form a "dot code". Not just any mark pattern can constitute a codeword, however, each codeword belongs to a specific family or set of mark patterns that conforms to a particular descriptive rule which governs a characteristic of each mark pattern, for instance, a rule about the width of each mark and the total width of each mark pattern. The codewords in any two adjacent rows are written in mutually exclusive subsets of the mark-pattern set (although in some embodiments the union of the subsets is not exhaustive of the set itself). In particular, each subset of the mark-pattern set is defined so that it includes as valid codewords for that subset, only those mark patterns that satisfy certain discriminator-

function criteria. Such a two-dimensional bar code is able to achieve storage of up to 1 kilobyte of memory within an area of one to four square inches which represents approximately 250 English words--about the size of a page or screen display. As an informational unit, such a unit is well suited for many applications of the present invention. U.S. Patent No. 5,504,322 describes such a two-dimensional bar code in greater detail and is hereby incorporated by reference.

Additional applications for the electromagnetic wave emissive machine-readable snippet 10 of the present invention are illustrated in Figs. 4-6 in the form of a money order, passport and shipping label, respectively. These applications are merely intended as examples of potential uses for the present invention and as such represent only a small subset of applications which would benefit from the many security advantages provided by the present invention.

One embodiment of the present invention comprises utilizing machine readable symbols printed on the secure document in order to ensure the authenticity of the blank secure document or stock. Physical parameters and characteristics of the stock such as the wavelength of light required to excite the coating to a predetermined emission spectrum; the emission spectrum of the coating for instance, the wavelength of light emitted upon exposure to a predetermined source of electromagnetic energy, etc.; manufacturing run identification or stock number; identification of the printer used to lithograph the stock, and a template or identification of quantity, location, size and characteristics of the coated areas appearing on the secure documents in order to guide and align the reader,

//

scanner and printer during the generation and verification phases. Such information may be applied anywhere on the secure document, (within the coating or outside the coating) however, application within the coating will yield additional protection against intentional or unintentional alteration by more readily disclosing alterations to the machine readable symbols.

Such information may be optionally encrypted, compressed, encoded into machine-readable symbols and applied by the manufacturer or lithographer responsible for applying the coating to the stock. For instance, the information may be encoded in micro PDF represented by the absence of ultraviolet ink including the name of the printing facility, the location of the printing facility, the identification number of the printing machine, the customer's name, the date of the printing run, and the number of UV snippets appearing on the document. Alternatively, the manufacturer of the stock could supply relevant information to a service bureau that would optionally encrypt, compress and encode the information into machine readable symbols and return the symbols to the manufacturer of the stock for application to the stock. In addition, the issuer of the secure document could optionally encrypt, compress and encode this information into machine readable symbols and apply the symbols to the stock if this information were made available in some way such as on the packaging of the stock which could be sold comprising a variety of different values for these parameters. The machine-readable symbol could take the form of micro PDF or could even be alphanumeric representation requiring scanning by Optical Character Recognition (OCR) techniques. The process of verifying authenticity of the stock is described in detail in section (C) below under the subheading entitled

"Verification Process", however, it essentially involves a comparison of the actual physical parameters and characteristics of the stock as obtained through physical manipulation of the stock (intrinsic verification) or via remote and/or local databases (extrinsic verification) to the data content of the machine readable symbols appearing on the stock. If the two are substantially the same then the authenticity of the stock has been verified. Thus, this embodiment (which may be combined with the embodiment described in section (I)(C) immediately below) provides a first level of authentication which verifies the authenticity of the stock without regard to additional information either contained on the face of the secure document or in corresponding locations of relevant local and remote databases.

Figs. 7A and 7B illustrate a flowchart which describes a detailed approach to the generation and verification of a secure document utilizing the electromagnetic wave emissive machine-readable snippet 10 of the present invention. In step 40 a blank secure document is manufactured comprising secure portions which are coated, impregnated or otherwise treated with a substance exhibiting a predetermined and specific spectral emission characteristics (emission of electromagnetic radiation of a wavelength in the range of 539-549nm) in response to exposure to electromagnetic radiation of a specified wavelength (ultraviolet light). These secure portions may also be referred to as ultraviolet snippets or a coating. The secure document could be in the form of money orders, gift certificates, passports, deeds, wills, licenses, packaging labels, negotiable instruments, titles, tickets, letters traveler's checks, food stamps or any other document for which secure verification of authenticity would be a

useful attribute. A user would then insert the blank secure document into a printer and invoke a program on a computer in step 44 which is adapted to encode information entered by the user into machine-readable symbols suitable for printing on top of the ultraviolet snippet. Typical information which the user might enter during step 46 in order to authenticate the document comprises the following:

1. biometrics (e.g., fingerprints by scanning or otherwise capturing an image of the fingerprint and digitizing it prior to encoding it in machine readable symbols); and
2. infometrics such as a birthdates, social security numbers, personal identification numbers (PIN's), demographics of those in the chain of negotiation, signatures (e.g., digital signatures or a digitized version of a handwritten signature such as that disclosed in U.S. Patent No. 5,138,140, hereby incorporated by reference), identification of financial institutions, payees, amount to be paid, drawer banks, and other human-readable and machine-readable information contained on the secure document as well as information contained in relevant local and remote databases.

The information entered by the user is optionally encrypted during step 48, optionally compressed during step 49 and encoded into machine-readable symbols during step 50 by any of the numerous techniques well known in the art. The machine-readable symbol is then printed on the secure

document in step 52. The user then completes the remaining areas on the secure document by hand or keyboard entry into the personal computer in step 54 and issues the secure document in step 56. This essentially ends a secure document generation phase of the process utilizing the electromagnetic wave emissive machine-readable snippet 10 of the present invention. The generation process described above could alternatively or in addition be performed by the printer who prints information on the check after the lithographer coats the check but before the user who issues the check.

At this point the secure document is ready to be issued, distributed, transferred or stored until needed. For instance if the secure document takes the form of a check, passport, or shipping label it may be transferred to a retail establishment, customs authority, or shipping company, respectively, which then performs intrinsic and/or extrinsic verification upon the secure document.

The secure document verification phase begins with insertion of the secure document into a scanner that scans both the machine-readable symbol as well as the human-readable information content of the secure document in step 60. Data content contained in the scanned machine-readable symbol is then decoded in step 58, decompressed in step 61 and decrypted in step 62 if the machine-readable symbol was compressed and encrypted during the secure document generation phase. The information content found in the human-readable information on the secure document and the data content found in the machine-readable symbol on the secure document may then be displayed in order to enable verification in step 66 by comparison between them or automatically verified without human invention. If the

comparison results in a match between the data content of the machine-readable symbol and the information content of the human-readable information then the secure document will have successfully completed the secure document verification phase. An unsuccessful match indicates an error in the secure document generation phase or a fraudulent alteration of the secure document thereafter. In addition the comparison may also take into account information obtained via outband resources or that information not obtained through inspection of the physical document but rather through queries of local or remote databases. For instance, information that would typically not appear on the face of the document would be digitized images of fingerprints, birthdates, mother's maiden names, etc.

The comparison step 66 specifically involves a two step process. The first step subjects the ultraviolet snippet to a predetermined wavelength of light. The actual spectral emission characteristics of the ultraviolet snippet are then captured, analyzed and verified against a set of expected spectral emission characteristics, and if the two are within a predetermined tolerance or range, then the ultraviolet snippet will be considered to be authentic. The set of expected spectral emission characteristics might be predetermined and fixed in the comparison step 66 in advance, transmitted via outband resources such as local or remote databases specifically for the verification phase or contained within the machine-readable symbol as suggested in section (I)(B) above. In this way a physical measurement (i.e. the expected spectral emission characteristics) is taken, the results are reduced to a data element (i.e., a digital value which represents the expected wavelength of light emitted from the ultraviolet snippet) and the data element is represented in the modulation of the physical

variable (i.e., the expected wavelength of emitted light is encoded and optionally encrypted and compressed in machine-readable symbol which is applied to the secure document of the present invention).

The second step of the comparison involves verification of the data content of the machine-readable symbol (which is decoded and optionally decrypted and decompressed from the machine-readable symbol) against the information content of the human-readable information on the secure document as well as additional information made available to the verification process via local and remote resources and databases. For instance, by digitizing the drawer's signature (via means disclosed in U.S. Patent No. 5,138,140) and encoding it into machine-readable symbol the typical signature card which is kept on file for each of the customers of a financial institution could be merged with the negotiable instrument thereby providing additional means with which to ensure the authenticity of the negotiable instrument.

An additional embodiment of the present invention is illustrated in Fig. 12 wherein a secure document 146 comprises the same zones covered with fluorescent coating ("UV snippets") as those illustrated in Fig. 1. However, in the check 146 one or more of the UV snippets have been printed with machine-readable symbols 148 in addition to the handwritten or printed indicia. The machine-readable symbols 148 are not restricted to being printed within the UV snippets, however, locating them there will provide the added benefit of security against alterations such as erasures. Figs. 13A-C illustrates a flow chart of a method to create, issue and verify such secure documents as the check 146 illustrated in Fig. 12.

The first step in the flowchart of Fig. 13A is to manufacture a blank secure document in step 150 which may comprise a negotiable instrument such as the check 146, money order, gift certificate or any document which would benefit from increased security against alteration and verification of authenticity. A user or issuer then completes the secure document by hand or machine in step 152 and invokes an issuing hardware/software package which could run on a personal computer in order to encode information into machine-readable symbols in step 154. The completed secure document is then inserted into the issuing hardware/software package or scanner in step 156 which scans the handwritten or printed indicia within the UV snippets and prepares a bit map comprising pixel coordinates which digitally describes the relative location of the handwritten or printed indicia with respect to the UV snippet in step 158. The scanner is guided by the UV snippet, which defines the area of interest and indicia to be scanned. Limiting the area of interest to the UV snippet reduces the probability of misreads due to dirt, dust and other environmental agents and factors which appear on the face of the secure document as well as imperfections in the blank secure document or stock which are not critical to the verification process. An additional advantage of limiting the field of interest to the UV snippets is that the overall speed of the scanning process is increased by reducing the area that is to be scanned.

The process of creating the bit mapped image of the UV snippets and other techniques involved in the capture and transmission of digital images such as compression and reconstruction are discussed in R. Dorf, Electrical Engineering Handbook 329-345 (1993), which is hereby

incorporated by reference. The imaging process essentially involves sampling the UV snippet by superimposing a grid over the UV snippet and examining the energy output from each box or pixel of the grid with a sensor. The output from each box is then converted to an electrical signal. A quantization process assigns a number to each of the electrical signals. The result of the quantization process is a bit map or a matrix of numbers that digitally represent the scanned image.

It must be decided whether the information encoded in machine-readable symbols should be the bit map itself or some indirect representation of it such as a cyclic redundancy check sequence (CRC), checksum, or hash function in decision 160. If the bit map will be used as the basis of the machine-readable symbol then the bit map is optionally encrypted, optionally compressed and encoded into machine-readable symbols (such as the two dimensional bar code illustrated as the machine-readable symbol 148 in Fig. 12) in steps 162, 164, and 166, respectively. However, if the bit map is not used then the hash function, checksum or an equivalent algorithm well known in the art is applied to the bit map in order to derive a distinguishing output which is optionally encrypted, optionally compressed and encoded into machine-readable symbol in steps 168, 170, and 172, respectively. After the machine-readable symbols have been printed on the secure document in step 174 it is issued in step 176. Thus, the machine-readable symbols function as a "Watermark" which verifies the authenticity of handwritten as well as machine-printed indicia on the secure document according to the relative position of such indicia with respect to a predetermined UV snippet.

The receiver of the secure document or one who desires to intrinsically or extrinsically verify its authenticity scans the UV snippets on the secure document by inserting the secure document into a verification software/hardware package in step 178 which will decode the machine-readable symbols in step 180. If the information encoded into machine-readable symbols is a bit map then it is optionally decompressed, optionally decrypted, decoded and compared with the bit map of the indicia appearing on the face of the secure document within the UV snippets in steps 184, 186, and 188, respectively. However, if the information which has been encoded into machine-readable symbol is not a bit map then the information is optionally decompressed, optionally decrypted, decoded and compared with the CRC sequence, checksum, hash function or substantially similar information derived from the bit map of the indicia appearing on the face of the secure document in steps 190, 192, and 194, respectively. Based upon the results of the comparison in steps 188 or 194, if the values are equivalent the authenticity of the secure document is indicated and the secure document is without material alteration to the handwritten or printed indicia in step 198 and thus intrinsic verification has been successful. However, if the values compared in steps 188 or 194 are not equivalent then the secure document is indicated as not authentic and/or comprising material alterations in step 200. Alternatively, or in addition to intrinsic verification the verifier may compare the scanned information to a relevant local or remote database in order to extrinsically verify the secure document.

Fig. 14 illustrates an embodiment of an issuing hardware package 202 and a verification hardware package 204 for implementing the method illustrated in Figs. 13A-C. A

blank secure document or stock 206 is completed by hand or machine yielding a completed document 208. The completed document 208 is inserted into an issuing scanner 210 in order to capture an image of the handwritten and/or machine printed indicia appearing thereon. This image is used by an issuing computer 212 in developing a bit map and/or derivative thereof by techniques well known in the art and described above. Upon optionally encrypting, optionally compressing and encoding the bit map and/or derivative thereof into machine-readable symbols the issuing computer 212 provides an issuing printer 214 with appropriate information to enable the issuing printer 214 to print machine-readable symbols representative of the bit map and/or derivative thereof on the completed document 208, which has been inserted into the issuing printer 214. A watermarked document 216 comprising machine-readable symbols is then ready for secure issuance, circulation, storage or verification.

In order to verify the watermarked document 216 it is inserted into a verifying scanner 218 which scans the UV snippets, thereby obtaining an image of indicia appearing on the watermarked document 216. A bit map and/or derivative thereof is developed from the image and compared to the machine-readable symbols that have been optionally decompressed, optionally decrypted and decoded in a verifying computer 220. If the components of this comparison are substantially equivalent then the watermarked document 216 has been successfully verified.

An additional embodiment of the two-phase imaging watermark process is illustrated in Fig. 12 in the alphanumeric amount zone 20 as an additional machine readable symbol 149. As illustrated in Fig. 15, after

applying the first machine readable symbol 148 by the method described above and in the flow chart of Figs. 13A-C the additional machine readable symbol 149 may be applied to any or all zones on the secure document in substantially the same manner, except that the additional machine readable symbol 149 will now reflect the presence of the first machine readable symbol 148 as well as any prior machine readable symbol. Any number of machine readable symbols 149 may be recursively placed on the secure document (representing the indicia within a zone and any or all prior machine readable symbols already printed in the zone) in order to describe any one or more coated areas or UV snippets as shown in steps 224 and 226, thereby yielding a mult-level watermarked document 228 (comprising in the case illustration three levels of security against alteration). This method enables a variable number of levels of security to be applied as required for any particular application. The verification phase will be required to start with the last machine readable symbol applied and proceed in reverse order of application, thus ignoring or deleting some or all machine readable symbols from the current image according to a predetermined sequence which were already verified in prior steps (or intentionally ignored at a particular level) since these symbols would not have been part of the image during the development of the current machine-readable symbol. Therefore, if a fraudulent alteration of the secure document is made, it must be reflected in some or all subsequent levels of machine readable symbols which have been generated with an image comprising the altered area. Variations on this concept may comprise including a predetermined subset of the previously applied machine readable symbols applied in the image represented by the current machine readable symbol being applied.

An additional advantage gained in using the watermark process is that since an image of the secure portions of the document has been encoded in machine-readable symbol any alterations, including not only erasures, but also additions to the indicia will be detected during the intrinsic and extrinsic verification processes.

Whereas the embodiments described above have focused upon methods of verifying the authenticity of the secure document by comparing information found on the face of the secure document with machine readable symbols also found on the face of the secure document (intrinsic verification), the following embodiments in the transactional tracking section utilize the self-verification method in addition to verification of the secure document by comparison to relevant databases either remote or local to the point of verification (extrinsic verification) and the two-stage imaging or watermark process described above. Fig. 8 illustrates an application of the electromagnetic wave emissive machine-readable snippet 10 of the present invention which essentially provides a payor bank 80 with an additional amount of time during which to decide whether to dishonor or finalize payment on a check. A holder 82 presents a secure document or check (having been prepared using the methods described above) to a depository bank 84 and a provisional credit (a credit that may be revoked prior to final payment of the instrument upon finding insufficient funds for payment, material alteration of the instrument or other deficiencies in the instrument) will be given to the holder 82. The check is then placed with others for delivery to an intermediary bank or clearing house 86, sorted by the payor bank 80 and totaled. The checks are then delivered to an intermediary bank 86 and given to an agent of the payor bank 80 and the provisional credit will

be entered. The checks are delivered to the payor bank 80, which determines their authenticity by verifying the checks against themselves (intrinsic verification as described above in section (I)) as well as against a positive pay file (extrinsic verification). If the payor bank 80 successfully verifies the check, both intrinsically and extrinsically, then the check is paid and all provisional credits are made final (or in the terms of the banking industry, "firmed up"). However, if the check is not successfully verified then it is dishonored, returned with the appropriate notations and the provisional credits are revoked at the clearing house 86 and the depository bank 84.

Under the Uniform Commercial Code §§ 4-213(1)(d), 4-301, and 4-302, which governs the check clearing process, if the payor bank 80 has already made a provisional credit for the check presented (as is the case with checks presented by the clearing bank 86) payment on that check becomes final if the provisional credit is not revoked prior to midnight of the banking day following the banking day of receipt. Upon final payment, the payor bank 80 becomes accountable for the amount of the check and generally has no recourse to avoid payment. Therefore, the payor bank 80 has only a limited time within which it must determine whether to pay a check or dishonor it. Since much of this time is used in transporting the physical check to the payor bank 80, very little time is remains for the decision making process.

If the check comprises the electromagnetic wave emissive machine-readable snippet 10 of the present invention, then either the depository bank 84 and/or the intermediary bank 86 could intrinsically verify the authenticity of the check utilizing the methods described

above in section (I). Alternatively, or in addition to intrinsic verification the depository bank 84 and the intermediary bank 86 could extrinsically verify 87 the authenticity of the check via a request to the payor bank 80, which would provide the intermediary bank with relevant information comprising the drawer's name, account number, check number, amount to be paid, etc. in order to extrinsically verify the same information appearing on the face of the check. The results of the verification phase are then forwarded to the payor bank 80 and/or the intermediary bank 86 in advance of the physical check in the form of an advance pay file 88. The advance pay file 88 comprises all of the human-readable information content and machine-readable data content which was obtained via direct inspection and scanning of the physical check by the depository bank 84 and/or the intermediary bank 86 two to three days in advance of an opportunity by the payor bank 80 to do so. Thus, the need to provide banks with a greater number of days to reconcile provisional credits is essentially eliminated since receipt and inspection of the physical check by the payor bank 80 is no longer required in order to verify authenticity of the check.

Fig. 9 illustrates a method for circulating a secure money equivalent such as money orders, gift certificates, etc. comprising the electromagnetic wave emissive machine-readable snippet 10 of the present invention. An issuer 100 sells a secure money order 104 comprising the electromagnetic wave emissive machine-readable snippet 10 to a consumer 102 in exchange for cash or a consumer cash equivalent 106. The additional functional responsibilities of the issuer 100 comprise the following:

1. marketing and sale of secure money orders 104;
2. reconciliation of information regarding the sale of secure money orders 104 to sales proceeds;
3. deposit of sales proceeds with an issuer's financial institution 128;
4. providing service to the consumer 102;
5. overseeing the maintenance of hardware and software used in the sale of secure money orders 104;
6. maintaining the quality of service by secure money order 104 issuing personnel and equipment; and
7. ordering consumables (e.g., ordering forms and displays media).

The consumer 102 issues the secure money order 104 in exchange for goods, services or a payee consideration 108 from a payee 110 of the consumer's choice that subscribes to the system of circulating secure money equivalents of the present invention. The payee 110 presents the secure money order 104 to a depository financial institution 112 in exchange for cash, a provisional credit on the payee's account or some other form of depository financial institution cash equivalent 114.

The depository financial institution 112 then presents the secure money order 104 to a clearing financial institution 116 in exchange for a provisional credit or some other form of clearing financial institution cash equivalent 118. Upon the initial sale of the secure money order 104 by the issuer 100, the issuer 100 transmits sales information 120 to a centralized service bureau 122 via outband

resources (mail, Internet, secure modem, etc.) which comprises such information describing the transaction as the date, time, amount, consumer identification, serial number and other identifying characteristics of the secure money order transaction and the service bureau 122 acknowledges its receipt of the sales information. Thereafter the service bureau 122 transmits a positive pay file 124 comprising information obtained from the transmitted sales information and a list of rejected items which should not be paid to the clearing financial institution 116 and perhaps additional relevant information appended by the service bureau 122. Based upon the information contained in the transmission of the positive pay file 124 the clearing financial institution 116 determines whether or not to pay the depository financial institution 112. The clearing financial institution 116 then transmits a paid items file 125 to the service bureau 122 comprising a list of those secure money orders 104 paid as well as additional relevant information describing the conditions under which payment was made.

Additional functional responsibilities of the service bureau 122 comprise the following:

1. issuance of debit instructions to the issuer's financial institution 128;
2. issuance of credit instructions to the clearing financial institution 116;
3. provision of customer support to the issuer 100, payee 110 and depository bank 112;
4. maintenance of quality control for secure money order issuance;
5. provision of all consumables;

6. installation and maintenance of all on-site hardware and software;
7. balancing and reconciliation of each step of the circulation process;
8. generation of on-line and printed reports for consumers 102; and
9. identification and return of all rejected secure money orders 104 within a predetermined period of time.

On a regular basis (daily) the issuer 100 will reconcile the consumer cash equivalent 106 received from the consumer 102 with the secure money orders 104 sold and will deposit an issuer's sales proceeds 126 which represents the gross sales receipts for the sale of secure money orders 104 into the issuer's financial institution 128. At the direction of the service bureau 122 the issuer's financial institution 128 will pay the clearing financial institution 116. The clearing financial institution 116 provides the clearing financial institution cash equivalent 118 to the depository financial institution 112 in exchange for the secure money order 104. The circulation process is complete when the clearing financial institution 116 transmits secure money orders 104 which have been paid or rejected to the service bureau 122 for identification and warehousing. The depository financial institution 112 has the option of seeking recourse against the consumer 102 or "writing-off" secure money orders 104 which were incorrectly paid as a loss.

Additional functional responsibilities of the clearing financial institution 116 comprise the following:

1. receipt of cash letters accompanying the secure money orders 104 from the depository financial institution 112;
2. verification of information obtained from the Magnetic-Ink Character Recognition (MICR) code; and
3. processing of returned secure money orders 104.

As an additional means of verification for the secure money order 104 the payee 110 and/or the depository financial institution 112 and/or the clearing financial institution 116 may request extrinsic verification as shown by reference numeral 130 of the authenticity of the secure money order 104 from the service bureau 122 via comparison of information in a positive pay file 124 from the service bureau 122 with information obtained from physical inspection and scanning of the secure money order 104. Alternatively, or in addition to this authentication technique, the payee 110, the depository financial institution 112 and/or the clearing financial institution 116 may perform intrinsic verification upon the secure money order 104 using methods described in section (I) above by verifying the authenticity of the ultraviolet snippet (stock verification) and comparing the data content of the machine-readable symbol with the information content of the human readable information on the secure money order 104) as shown by reference numeral 132.

Fig. 10 illustrates the services provided by the service bureau 122 to the other entities involved in the circulation of the secure money order 104. Specifically, support services will be provided by the service bureau 122 to the issuer 100 in order to service the consumer 102 with

inquiries regarding payments and requests for copies of secure money orders which were paid as well as stop payments. The issuer 100 transmits sales information to the service bureau 122 in a batch flow manner. The service bureau 122 also responds to requests by the payee 110 and/or the depository financial institution 112 for confirmation of the authenticity of the secure money order 104 (encashment authorization service inquiries 130) in real time.

In the process for circulating secure money orders 104 described above the seller of secure money orders is given the opportunity to become the issuer 100 of his own secure money orders 104 by action of the board of the directors of the issuer 100. Once the board of directors determines that an issuer 100 will issue secure money orders 104 an application is made to the state government for a local license and a bond. Upon posting the bond and obtaining the license, the issuer 100 is able to promote and issue its own secure money orders 104 without concerns regarding inventory controls and audits, safekeeping facility requirements, or theft of blank financial paper. The service bureau 122 may decide to offer incentives to help underwrite the marketing costs of new issuers 100 in return for a larger percentage of the long term float and escheat funds from secure money orders that have not been redeemed.

The sale of secure money orders 104 can be performed at any suitable location such as a cash register, a check-out line, or a customer service area. In such a situation a customer service representative enters a unique personal identification and a password into a keypad or other terminal entry device associated with a computer. In response, an issuing system accesses a security-cleared,

pre-authorized secure money order input screen in which the amount to be assigned to the secure money order is entered. Upon issuance, the issuing system generates the secure money order 104 and a receipt or the equivalent of an application form, which was completed by the consumer 102.

Figs. 17 and 18 provide greater detail regarding two embodiments for the transaction between the consumer 102 and the issuer 100 in issuing secure money orders and secure gift certificates, respectively. These embodiments are specifically intended for retail establishments in which the following characteristics are present:

1. a customer service desk or area is not available to conduct the issuance of secure documents;
2. cashiers are provided with a minimal level of training and wages while turnover is relatively high; and
3. the secure document issuing hardware, software and procedures may be integrated with existing point of sale configurations and procedures.

Fig. 17 illustrates the issuance of a secure money order which is first selected by the consumer in the display area and taken to the cashier much like any other product being purchased in a retail store. A serial and stock number would be imprinted on the secure money order in machine readable code along with the SKU and UPC of the prior art. The secure money order would, for instance, be enclosed in clamshell wrapping and hung on a peg in a display rack. Also, a closed package with access through a visible envelope or cutaway portion may be used. The cashier would then scan the blank secure money order

automatically invoking software prompting the cashier or consumer to enter an amount, dollar value or denomination for the secure money order via a keyboard and display or other equivalent means of entry and acknowledgement well known in the art. Issuance information obtained by scanning the secure money order along with the amount provided (which may be fixed on the document or printed during the transaction by the cashier) is then transmitted to a merchant central database for recording and further processing. The issuance information along with optional additional information such as the time, date and location of issuance is then transmitted to the service bureau for recording, processing and verification against prior records regarding the printing of the secure money order (extrinsic verification). If the results of the verification are satisfactory, authentication information is transmitted back to the merchant central database for recording, processing and transmittal to the cashier. Upon receipt of the authentication information, the cashier will activate the secure money order by imprinting the desired denomination along with authentication information obtained from the service bureau in machine readable code using the methods described above via the cashier's register. The cashier then transfers the activated secure money order with a receipt for the transaction to the consumer, thus concluding the sale or issuance of the secure money order.

An alternative embodiment for the issuance of the secure money order, which is also illustrated in Fig. 17, involves the transfer of value via electronic means rather than by physical transfer of the document. The issuance process for the secure money order which initiates an electronic fund transfer would be substantially the same as that described immediately above, except that the consumer

would only receive a receipt for the transaction without the activated secure money order since the transfer is no need for the transfer of the physical document in the negotiation process.

Fig. 18 illustrates the issuance of a secure gift certificate, which is substantially the same as the secure money order embodiment illustrated in Fig. 17, except that gift certificates may optionally be available to the consumer in predetermined denominations making the entry of denominations unnecessary. Although possible, gift certificates would not typically involve the transfer of funds via electronic means.

The hardware requirements of the issuing system are modest and typically comprise the following:

1. a personal computer;
2. 64 megabytes of RAM;
3. a CD ROM drive;
4. a Hayes compatible modem (56 Kbps) for transmission of sales information 120 to the service bureau;
5. a laser printer (the specific manufacturer and model number of which may be required to be certified by the service bureau 122 in order to maintain quality of printing standards);
6. blank secure money order stock to be supplied by the service bureau 122; and
7. cartridge toner (which may be provided by the service bureau 122 in order to ensure print quality as well as the use of

special inks to further guarantee authenticity).

The software requirements of the issuing system comprise a customer on-site module to include sales, issuing logic, print routines, and telecommunications capabilities. In addition the software and hardware may comprise the following characteristics:

1. passwords and customer service representative identifications for controlling security levels and to protect levels of access and input to the issuing system at all times;

2. the ability to store a series of ascending, consecutive secure money order serial numbers unique to the issuer 100 and the location of the issuing system;

3. a display to control the issuance of the secure money order 104 which displays the value and quantity of each secure money order 104 to be issued;

4. print routines which depict the face of the instruments customized with an issuer's logo (subject to federal restrictions and guidelines for financial instruments), the Magnetic-Ink Character Recognition (MICR) code and the machine-readable symbol (according to specifications provided by the service bureau 122).

5. telecommunications capability comprising an ability to generate a sales information file do be transmitted to the service bureau (primarily via the Internet). As a back up mode, other Internet Access Providers could be utilized as auxiliary channels of access to the service bureau 122 via

telephone lines from the issuer 100 to the service bureau 122.

In order to initiate the issuing system the issuer 100 receives software designed to access an Internet access provider (e.g., MCI, MSN, or AT&T Worldnet) having local access. The software enables the issuer 100 to set up an account with the Internet Access Provider (IAP). Once the account is set up and the software has logged the issuing system onto the Internet, the software addresses itself to the website corresponding to the service bureau 122, which will not require additional input from the issuer 100. The software transfers the sales information file from the issuing system to the service bureau 122 once the software logs onto the service bureau website using security codes provided by the service bureau 122. When the transfer is complete, the service bureau 122 verifies that the sales information file has been received and transmits a formal acknowledgment back to the issuing system which is read by the issuer 100. Simultaneously, an Internet mail server at the service bureau 122 optionally transmits financial reports documenting status of the secure money order business (e.g., gross sales, net proceeds of sales, volume of sales, etc.) to the issuer 100.

To accommodate future expansion of the method of circulating secure money orders of the present invention operates in a "Many to One" mode. Similarly, current technology controlling the Internet permits a multitude of parties to communicate with a host computer simultaneously without a substantial degradation in performance. Therefore, by utilizing the Internet the service bureau 122 can dramatically increase the number of issuers 100

accessing the service bureau 122, while limiting the need for additional phone lines and support personnel.

The circulation method illustrated in Fig. 9 of the present invention will also permit operation in a "One to Many" mode which will enable the service bureau 122 to provide communication back to the issuer 100 in order to accommodate consumer service requests, general inquiries, stop payments, reporting, etc. Modifications to the software of the issuing system can be made available to the issuer 100 via E-mail, and therefore, worldwide customer service and support can be conducted efficiently and economically without sacrificing quality.

It is anticipated that issuers 100 will reconcile sales receipts with consumer cash equivalent 106 received at least once a day in accordance with internal procedures generated by the service bureau 122. Where reconciliation is performed manually, the issuer 100 must total all consumer application forms and generate from this total a daily settle form (DSF) summarizing the total sales, voids and fees (consumer cash equivalents collected). The total of the DSF's must equal the total cash or issuer's sales proceeds to be deposited with the seller's financial institution 128 for that particular day. Where reconciliation is performed automatically (by the issuing system), the issuer 100 is merely required to reconcile a summary output of the daily sales information for the issuing system versus the issuer's sales proceeds 126 to be deposited in the seller's financial institution 128.

The issuing system must record detailed sales information regarding the secure money orders 104 issued, cancelled (voids), and consumer cash equivalents 106

received in addition to maintaining comprehensive information regarding ongoing balances. This information is available both via a visual display as well as a printed copy. Daily totals are archived in a suitable database for historical and statistical tracking. The software is designed to enable future upgrade capability for conversion between international currencies.

An additional embodiment of the present invention involves an application to food stamps. Food stamps are generally issued by an entity administered by a government agency that must typically post reserve funds in an account that services and provides funds for the food stamps. These reserves are used to cover anticipated fraudulent redemption of food stamps and are extremely costly to maintain. However, if the method of providing secure documents were used with food stamps, then such a costly reserve could either be substantially reduced or eliminated entirely. Additional savings could be realized from the substantial reduction in fraudulent redemptions.

A typical distribution method for circulating secure food stamps 134 is illustrated in Fig. 11 which utilizes methods of intrinsic and extrinsic verification that are substantially similar to those discussed above with respect to secure money orders. A government authorized issuer 136 transfers the secure food stamps 134 to the consumer 102 based upon a predetermined set of eligibility requirements and transmits distribution information 142 to the service bureau 122. The consumer 102 then presents the secure food stamps 134 to the payee 110 in exchange for payee cash equivalent 108 that typically takes the form of necessities such as food. Prior to the exchange the payee 110 may intrinsically verify the authenticity of the secure

food stamp himself 132 and/or request confirmation of its authenticity 130 (extrinsic verification) from the service bureau 122. The payee 110 then transfers the secure food stamp 134 to either a redemption institution 138 which may be the government, an authorized private entity or the government issuer 136 in exchange for redemption institution cash equivalent 140 which typically takes the form of cash or credit to an existing account. The redemption institution 138 possesses the same options for verification of the secure food stamp, as did the payee 110. Upon redemption of the secure food stamp 134 the redemption institution 138 transmits payment information 142 to the service bureau 122. The redemption institution 138 transfers secure food stamps 134 which have been redeemed back to the government issuer 136 or another entity which provides the warehousing function. The government issuer 136 may also perform intrinsic verification upon the secure food stamp 134 as a prerequisite to its acceptance.

Another embodiment of the electromagnetic wave emissive machine-readable snippet of the present invention is in the creation of a "suspended electronic fund transfer (EFT)" embedded on a negotiable instrument. The term EFT is a generic term describing the transfer of funds, other than a transaction originated by check, draft or similar paper instrument, initiated through an electronic terminal, telephone or computer for the purpose of ordering, instructing or authorizing a financial institution to debit or credit an account. The term includes but is not limited to point-of-sale transfers, automated teller machines (ATM) transfers, pre-authorized debits and credits conducted through automated clearing houses (ACH), pre-authorized pay by telephone transfers, check verification and guarantee and check truncation and wire transfers. The term does not

include payments made by check, draft or similar paper instruments at an electronic terminal. ACH transfers are typically used by a number of popular money management software packages (e.g., Checkfree® and Quicken®). Such transfers are relatively inexpensive and clear in one to two days. Currently, the security against fraud is performed entirely by the underlying system (ACH) which confirms the transfer through the Federal Banking System.

In November 1978, Congress enacted the Electronic Fund Transfers Act as Title IX to the Consumer Credit Protection Act (15 USC §1693). In 1979, Regulation E, issued by the Board of Governors of the Federal Reserve System, was intended to implement and carry out the purpose of the Act (12 CFR Part 205). The purpose and rationale of the Act resulted from a finding by Congress that the use of electronic systems to transfer funds provided substantial benefits to consumers. It is the purpose of the Act to provide a basic framework establishing the rights, liabilities, and responsibilities of participant in the electronic fund transfer systems. The primary objective of the Act, however, was to provide rights for the individual consumer, and Regulation E is primarily intended to carry out that purpose. The underlying goal is to reduce the flow of paper instruments and transactions in order to eliminate or significantly reduce the time and cost involved in the collection process.

According to the Act the receiver of an electronic fund transfer is not permitted to finalize the transfer until the existence and sufficiency of funds to be transferred is confirmed. By applying the electromagnetic wave emissive machine-readable snippet of the present invention to embed an EFT authentication code or suspended

EFT within an ordinary appearing check the verification of the suspended EFT and availability of funds already set aside to accommodate the transfer can be accomplished substantially faster. The EFT authentication code essentially comprises a macro authentication code (MAC) or Data Encryption Standard (DES) key. For example, as illustrated in Fig. 16, the consumer 102 issues a check bearing the suspended EFT 230 to a payee 110 who then presents it to a depository bank 112. The depository bank 112 then sorts it, extracts the suspended EFT 230, verifies the authenticity of the suspended EFT (intrinsically 132 and extrinsically 130 via request to the service bureau 122) at which point the physical document may be discarded. The suspended EFT would then be submitted directly to the FEDNET for transfer of funds from one account to another. A detailed discussion of the terms used above appears in Special Issue: Electronic Money, IEEE Spectrum February 1997, which is hereby incorporated by reference.

A further advantage realized by the embodiments described above is that the supporting documentation (e.g., advance pay file 88, paid item file 125, payment information 142) which tracks the circulation of the secure documents while being an automatic byproduct of the process also satisfies the record-keeping requirements for escheatment recovery. Under state law a percentage (e.g., 85%) of funds in a payment system are permitted to escheat or revert back to the issuing entity upon remaining uncollected or unpaid for a predetermined time period (typically three to seven years depending on the state). In addition, the two-tiered approach to verification of secure documents described above as intrinsic and extrinsic verification, not only permits verification at the Point Of Sale (POS) and every other point in the circulation of the secure document, but also

provides a remote database (e.g., advance pay file 88, paid item file 125, payment information 142) which is substantially impossible to fraudulently alter in concert with and in the precise way that the secure document itself has been altered. Thus, if a discrepancy is discovered as a result of the extrinsic verification and/or the intrinsic verification processes the secure document will be labeled as fraudulent.

An additional embodiment using the authentication methods described in the Secure Document Generation and Transactional Tracking sections above is a travelling signature card which follows such documents as a negotiable instrument, traveler's check or credit card as illustrated in Fig. 19. It should be noted that such documents need not have and in fact should not have a human readable representation of the user's signature in order to substantially eliminate the potential for forgery. Any document that benefits from authentication of the user's signature at a location remote to the storage of the signature card by comparing it against a pre-signed signature card which is inaccessible to unauthorized users could be used advantageously with this embodiment. Such a document is imprinted with machine readable code comprising an optionally encoded and compressed bit map of the user's signature which has been signed on the signature card typically at the opening of the account or under equivalent circumstances well known in the art. In order to verify the user' signature on the document or card the merchant scans the document or card and associated hardware and software provides a visual image of the user's pre-signed signature from the bit map encoded on the document or card. The merchant then visually compares the handwritten signature of the person attempting to use the document or card with the

visual image derived from the bit map and if they are substantially similar the authentication is successful. Thus, information contained on the typical signature card travels with the document or card enabling those without access to the physical signature card to conduct signature analysis. This also allows a consumer to carry information typically contained only in the signature card without it being visibly apparent to a potential forger, as in the case of credit cards bearing signature blocks in the prior art.

Although the invention has been shown and described with respect to best mode embodiments thereof, it should be understood by those skilled in the art that the foregoing and various other changes, omissions and additions in the form and detail thereof may be made therein without departing from the spirit and scope of the present invention.

WE CLAIM:

1. A secure document comprising:
   a) a substrate;
   b) an ultra-violet snippet field coated over at least a portion of the substrate;
   c) a machine-readable indicia imprinted on the substrate, the indicia being encoded with data representing a physical characteristic of the document.

2. The secure document of claim 1 wherein the indicia is encoded with a physical characteristic of the ultra-violet snippet field.

3. The secure document of claim 2 wherein the physical characteristic of the ultra-violet snippet field comprises a wavelength of light required to excite the coating to a predetermined emission spectrum.

4. The secure document of claim 2 wherein the physical characteristic of the ultra-violet snippet field comprises a wavelength of light emitted upon exposure to a predetermined source of electromagnetic energy.

5. The secure document of claim 2 wherein the machine-readable indicia is a bar code symbol that is imprinted substantially over the ultra-violet snippet field.

6. The secure document of claim 2 further comprising a plurality of fields populated with information suitable for use as a gift certificate.

7. The secure document of claim 2 further comprising a plurality of fields populated with information suitable for use as a money order.

8. The secure document of claim 2 further comprising a plurality of fields populated with information suitable for use as a check.

9. The secure document of claim 2 further comprising a plurality of fields populated with information suitable for use as a food stamp.

10. The secure document of claim 2, further comprising a plurality of data fields, the data fields comprising information regarding a transaction to be implemented by the document, the data fields comprising human-readable information substantially overlapping an ultra-violet snippet field.

11. The secure document of claim 10, further comprising a machine-readable indicia encoded with at least a portion of the human-readable information regarding a transaction to be implemented by the document.

12. The secure document of claim 2, further comprising a

data field comprising a secondary machine-readable indicia encoded with information specific to a user of the document.

13. The secure document of claim 12, wherein the information specific to a user of the document comprises biometric information of the user.

14. The secure document of claim 12, wherein the information specific to a user of the document comprises infometric information of the user.

15. A method of generating a secure document comprising

the steps of:

a) coating an ultra-violet snippet field over at least a portion of a substrate;

b) encoding a machine-readable symbol with data representing a physical characteristic of the document; and

c) imprinting the machine-readable indicia on the substrate.

16. The method of claim 15 wherein the indicia is encoded with a physical characteristic of the ultra-violet snippet field.

17. The method of claim 16 wherein the physical characteristic of the ultra-violet snippet field comprises a wavelength of light required to excite the coating to a predetermined emission spectrum.

18. The method of claim 16 wherein the physical characteristic of the ultra-violet snippet field

comprises a wavelength of light emitted upon exposure to a predetermined source of electromagnetic energy.

19. The method of claim 16 wherein the machine-readable indicia is a bar code symbol that is imprinted substantially over the ultra-violet snippet field.

20. The method of claim 16 wherein the machine-readable symbol is encoded and printed substantially contemporaneous with the coating step.

21. The method of claim 16 wherein the machine-readable symbol is encoded and printed substantially non-contemporaneous with the coating step by a secondary process.

22. The method of claim 16 further comprising the step of imprinting a plurality of data fields on the document, the data fields comprising information regarding a transaction to be implemented by the document, the data fields comprising human-readable information substantially overlapping an ultra-violet snippet field.

23. The method of claim 22, wherein the document further comprises a machine-readable indicia encoded with at least a portion of the human-readable information regarding a transaction to be implemented by the document.

24. The method of claim 16 further comprising the step of imprinting a data field on the document, the data field comprising a secondary machine-readable indicia encoded with information specific to a user of the document.

25. The method of claim 16, wherein the information specific to a user of the document comprises biometric information of the user.

26. The method of claim 16, wherein the information specific to a user of the document comprises infometric information of the user.

27. A method of verifying a secure document, the secure document comprising a substrate, an ultra-violet snippet field coated over at least a portion of the substrate, and a machine-readable indicia imprinted on the substrate, the indicia being encoded with data representing a physical characteristic of the document, the method comprising the steps of:

a) measuring the physical characteristic of the document;

b) scanning the machine-readable indicia;

c) decoding the data representing a physical characteristic of the document;

d) comparing the measured physical characteristic with the decoded physical characteristic; and

e) indicating the verification of the document when the comparison step provides results within a predefined tolerance.

28. The method of claim 27 wherein the indicia is encoded with a physical characteristic of the ultra-violet snippet field, and wherein the step of measuring the physical characteristic of the document comprises the step of measuring the physical characteristic of the ultra-violet snippet field.

29. The method of claim 28 wherein the physical characteristic of the ultra-violet snippet field comprises a wavelength of light required to excite the coating to a predetermined emission spectrum.

30. The method of claim 28 wherein the physical characteristic of the ultra-violet snippet field comprises a wavelength of light emitted upon exposure to a predetermined source of electromagnetic energy.

31. The method of claim 28 wherein the machine-readable indicia is a bar code symbol that is imprinted substantially over the ultra-violet snippet field, and wherein the step of scanning the machine-readable indicia comprises the step of scanning the bar code symbol with a bar code scanning device.

32. The method of claim 28 wherein the secure document further comprises a plurality of data fields imprinted thereon, the data fields comprising information regarding a transaction to be implemented by the document, the data fields comprising human-readable information substantially overlapping an ultra-violet snippet field, wherein

the document further comprises a machine-readable indicia encoded with at least a portion of the human-readable information, the method comprising the further steps of

scanning the machine-readable indicia to decode human-readable information, and

comparing the human-readable information on the document to the human-readable information decoded from the indicia.

33. The method of claim 28 wherein the document further comprises a data field imprinted on the document, the data field comprising a secondary machine-readable indicia encoded with information specific to a user of the document, the method comprising the further steps of

scanning the secondary machine-readable indicia to decode the information specific to a user of the document, and

comparing information obtained from a user of the document to the information specific to a user of the document decoded from the indicia.

34. A method for generating a watermarked secure document comprising the steps of:

a) coating an ultra-violet snippet field over at least a portion of a substrate;

b) executing the document by a user, the user entering information over at least a portion of the snippet field;

c) optically scanning the document in the area defined by the snippet field to obtain an

image of the information entered by the user over at least a portion of the snippet field;

d) encoding a representation of the scanned image into a machine-readable symbol; and

e) imprinting the machine-readable symbol onto the document.

35. The method of claim 34 wherein the information entered by the user is the signature of the user.

36. The method of claim 34 wherein the information entered by the user corresponds to a transaction with which the document is utilized.

37. The method of claim 36 wherein the information entered by the user corresponding to a transaction with which the document is utilized is a payment amount.

38. The method of claim 34 wherein the representation of the scanned image is a bit map comprising pixel coordinates that digitally represent the relative location of the scanned image.

39. The method of claim 34 wherein the representation of the scanned image is a checksum.

40. A method for verifying a watermarked secure document, the secure document comprising a substrate, an ultra-violet snippet field coated over at least a portion of the substrate, the snippet field having information entered by a user over at least a portion thereof, and a machine-readable symbol imprinted thereon, the machine readable

symbol being encoded with a representation of an image of the information entered by the user over at least a portion of the snippet field; the method comprising the steps of:

a) optically scanning the document in the area defined by the snippet field to obtain an image of the information entered by the user over at least a portion of the snippet field;

b) scanning the machine-readable symbol;

c) decoding the scanned machine-readable symbol to determine an expected representation of an image of the information entered by the user;

d) comparing the expected representation to the optically scanned image; and

e) indicating that the document has been verified when the results of the comparison step is within a predefined tolerance.

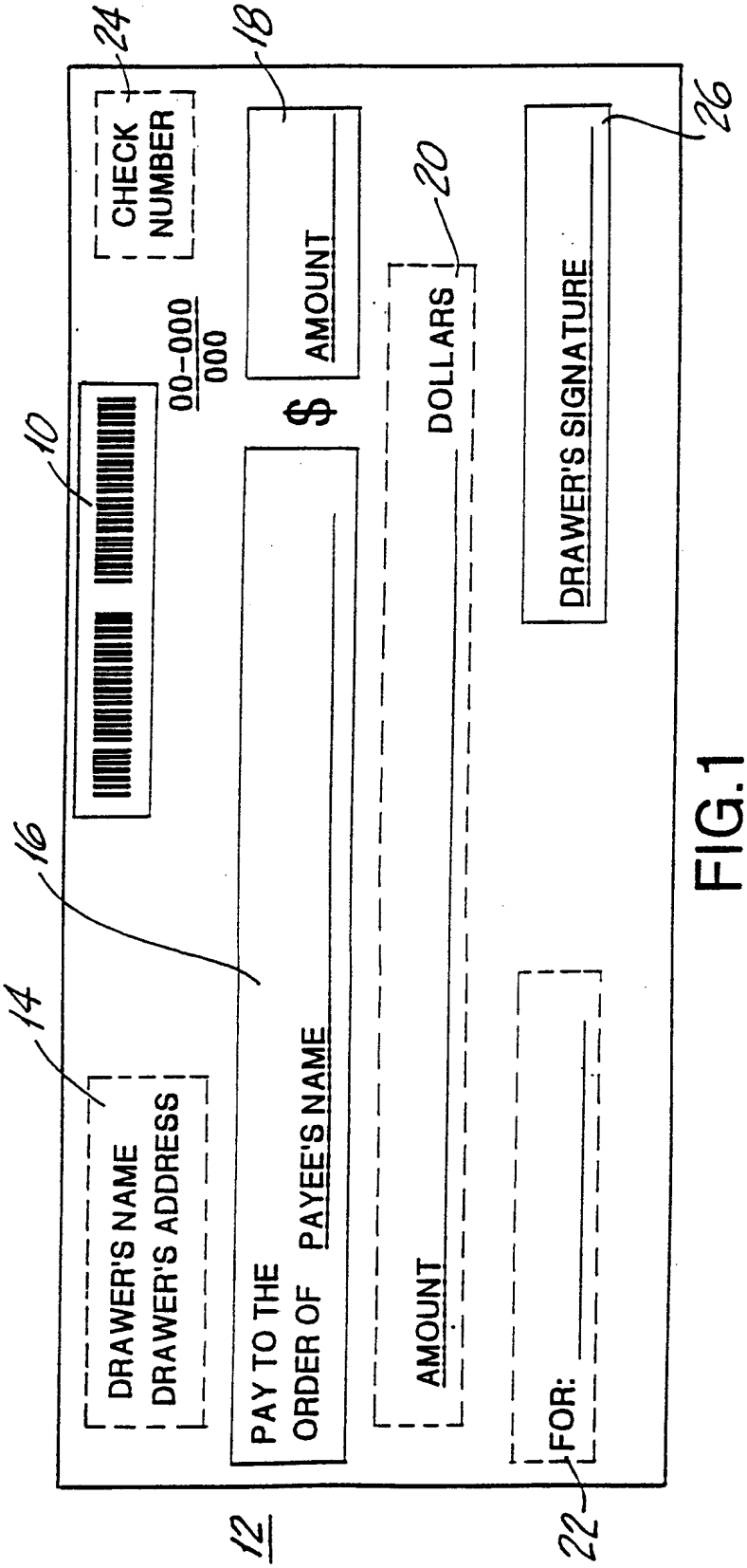

10
12
14
16
18
20
22
24
26
CHECK NUMBER
00-000/000
$ AMOUNT
DOLLARS
DRAWER'S SIGNATURE
DRAWER'S NAME
DRAWER'S ADDRESS
PAY TO THE ORDER OF PAYEE'S NAME
AMOUNT
FOR:

FIG.1

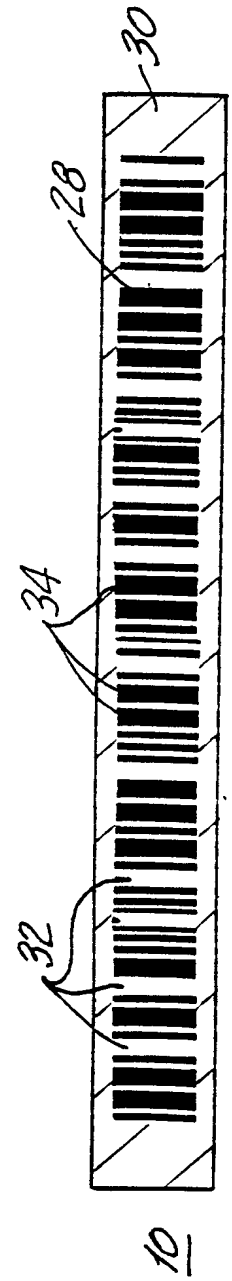

10
28
30
32
34

FIG.2

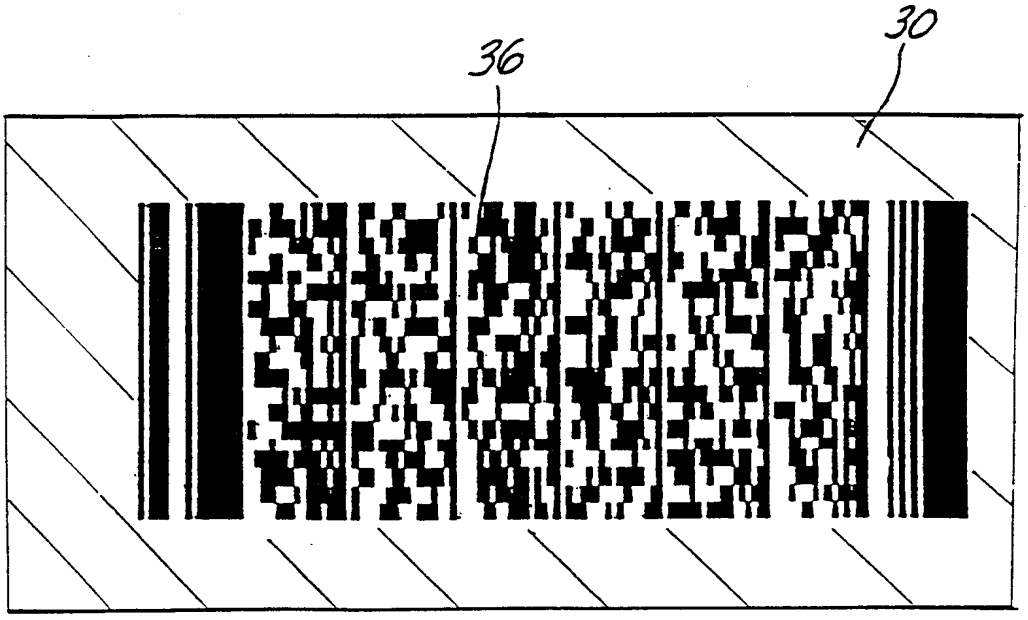


FIG.3

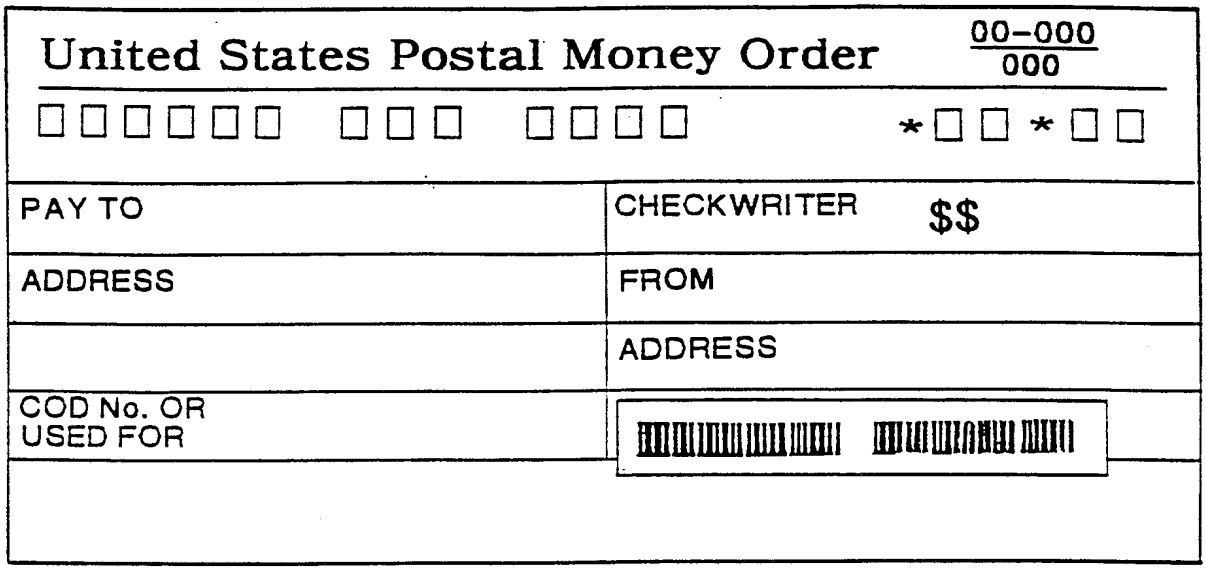

United States Postal Money Order
00-000
000
PAY TO
CHECKWRITER
$$
ADDRESS
FROM
ADDRESS
COD No. OR
USED FOR

FIG.4

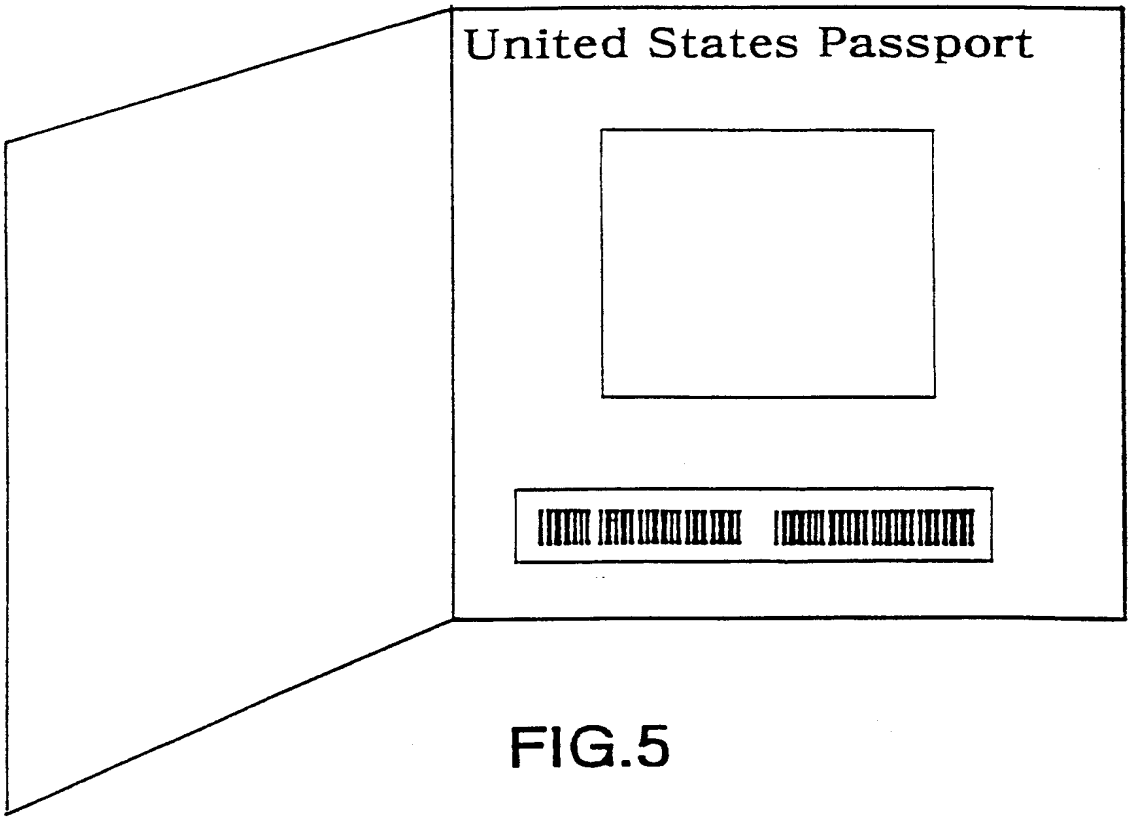

United States Passport

FIG.5

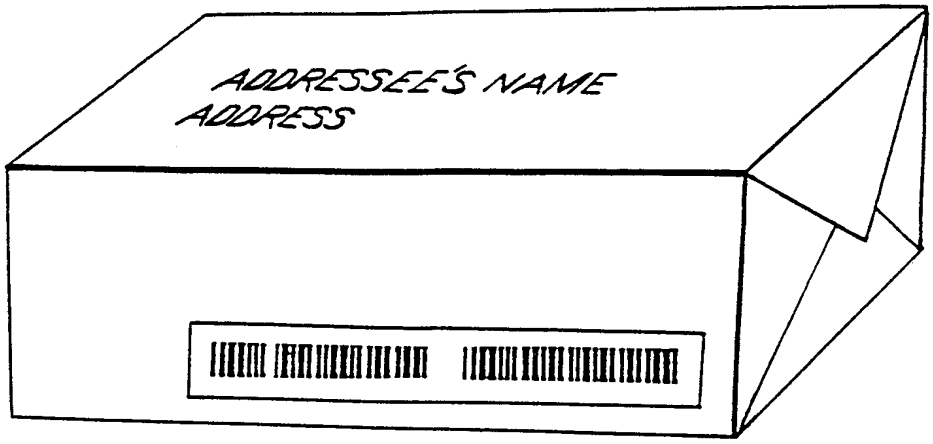


FIG.6

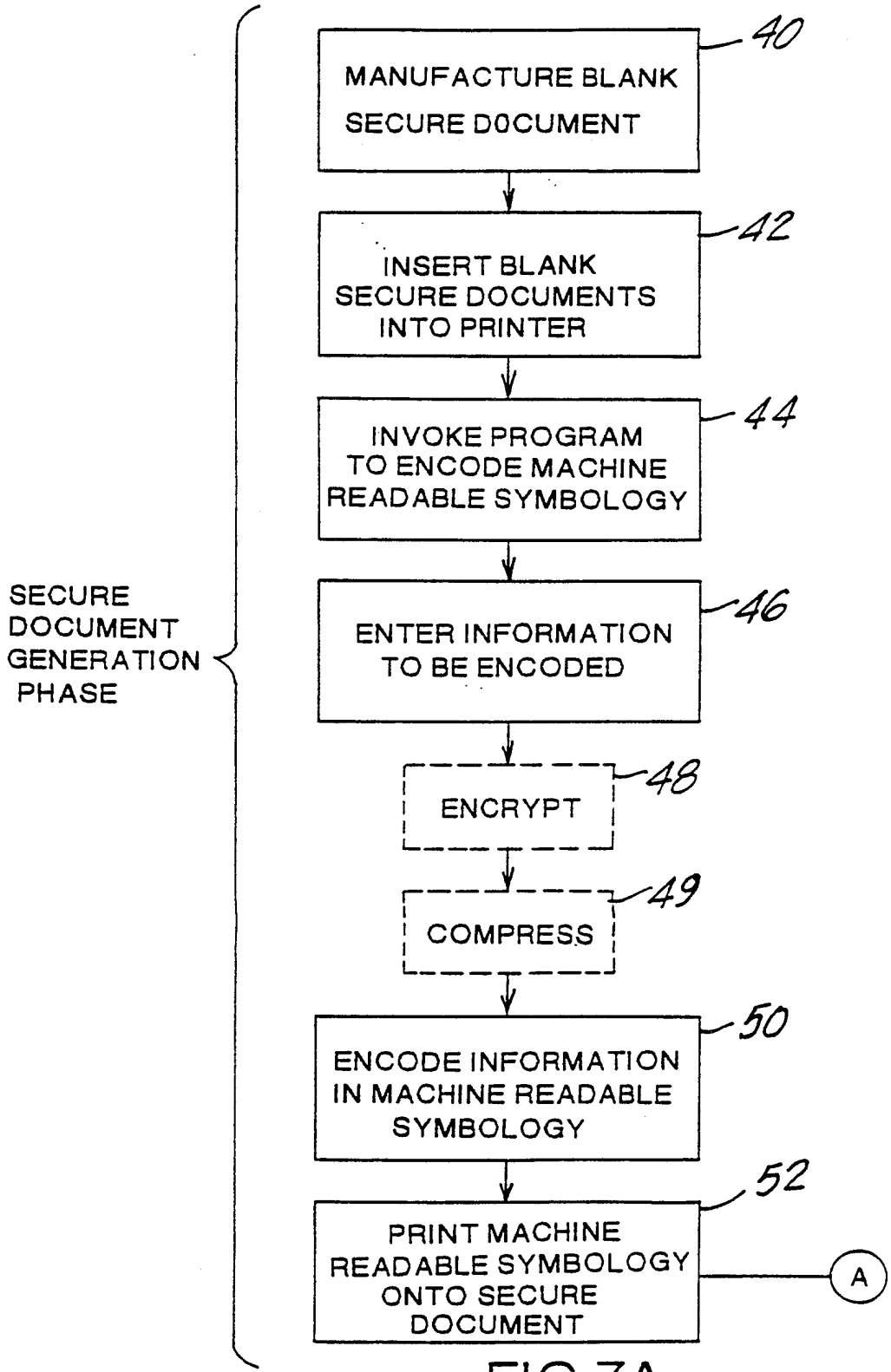

SECURE DOCUMENT GENERATION PHASE
MANUFACTURE BLANK SECURE DOCUMENT
40
INSERT BLANK SECURE DOCUMENTS INTO PRINTER
42
INVOKE PROGRAM TO ENCODE MACHINE READABLE SYMBOLOGY
44
ENTER INFORMATION TO BE ENCODED
46
ENCRYPT
48
COMPRESS
49
ENCODE INFORMATION IN MACHINE READABLE SYMBOLOGY
50
PRINT MACHINE READABLE SYMBOLOGY ONTO SECURE DOCUMENT
52
A

FIG.7A

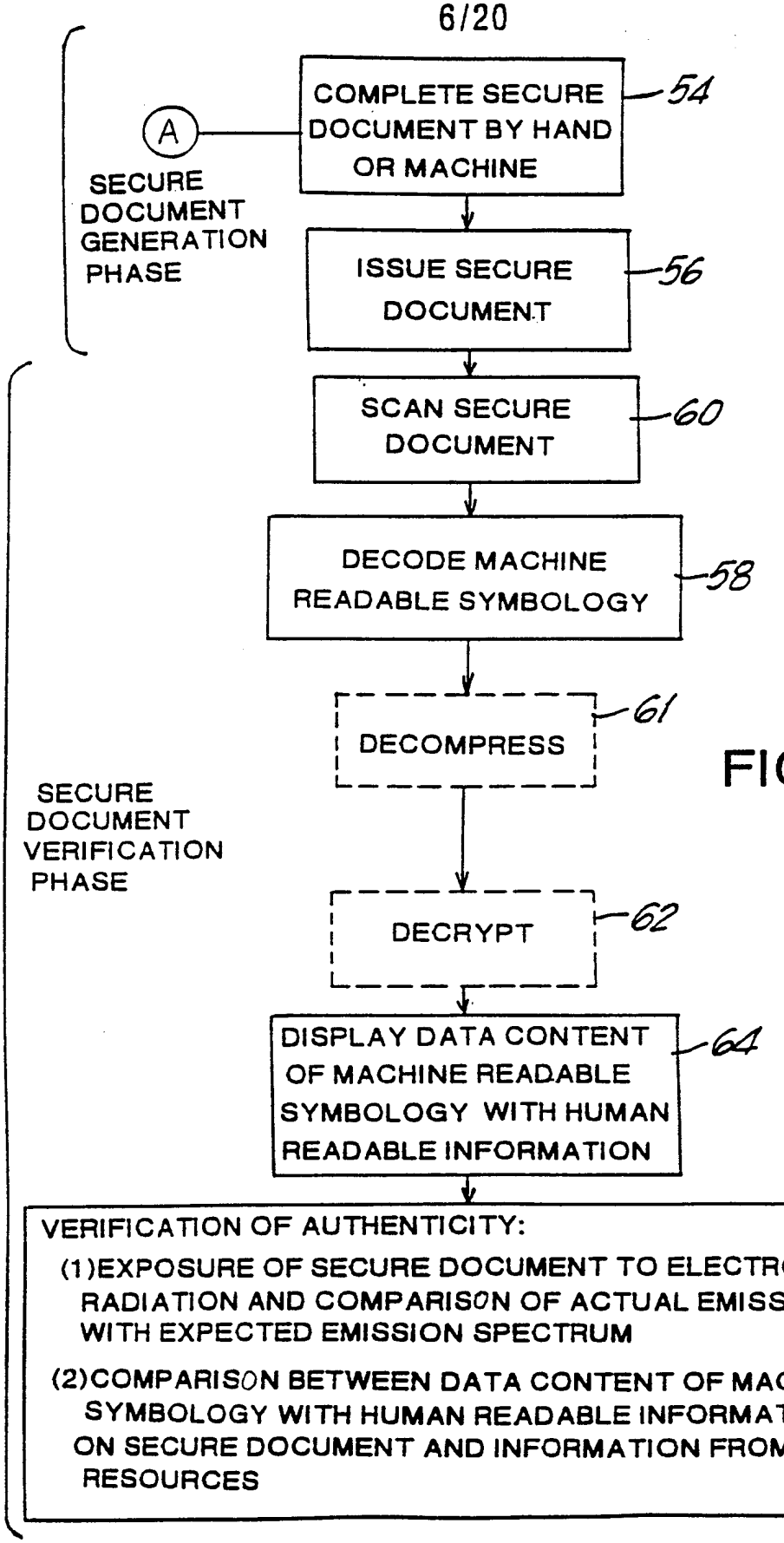

A
COMPLETE SECURE DOCUMENT BY HAND OR MACHINE
54
SECURE DOCUMENT GENERATION PHASE
ISSUE SECURE DOCUMENT
56
SCAN SECURE DOCUMENT
60
DECODE MACHINE READABLE SYMBOLOGY
58
DECOMPRESS
61
SECURE DOCUMENT VERIFICATION PHASE
DECRYPT
62
DISPLAY DATA CONTENT OF MACHINE READABLE SYMBOLOGY WITH HUMAN READABLE INFORMATION
64
66
VERIFICATION OF AUTHENTICITY:
(1)EXPOSURE OF SECURE DOCUMENT TO ELECTROMAGNETIC RADIATION AND COMPARISON OF ACTUAL EMISSION SPECTRUM WITH EXPECTED EMISSION SPECTRUM
(2)COMPARISON BETWEEN DATA CONTENT OF MACHINE READABLE SYMBOLOGY WITH HUMAN READABLE INFORMATION CONTENT ON SECURE DOCUMENT AND INFORMATION FROM OUTBAN RESOURCES

FIG.7B

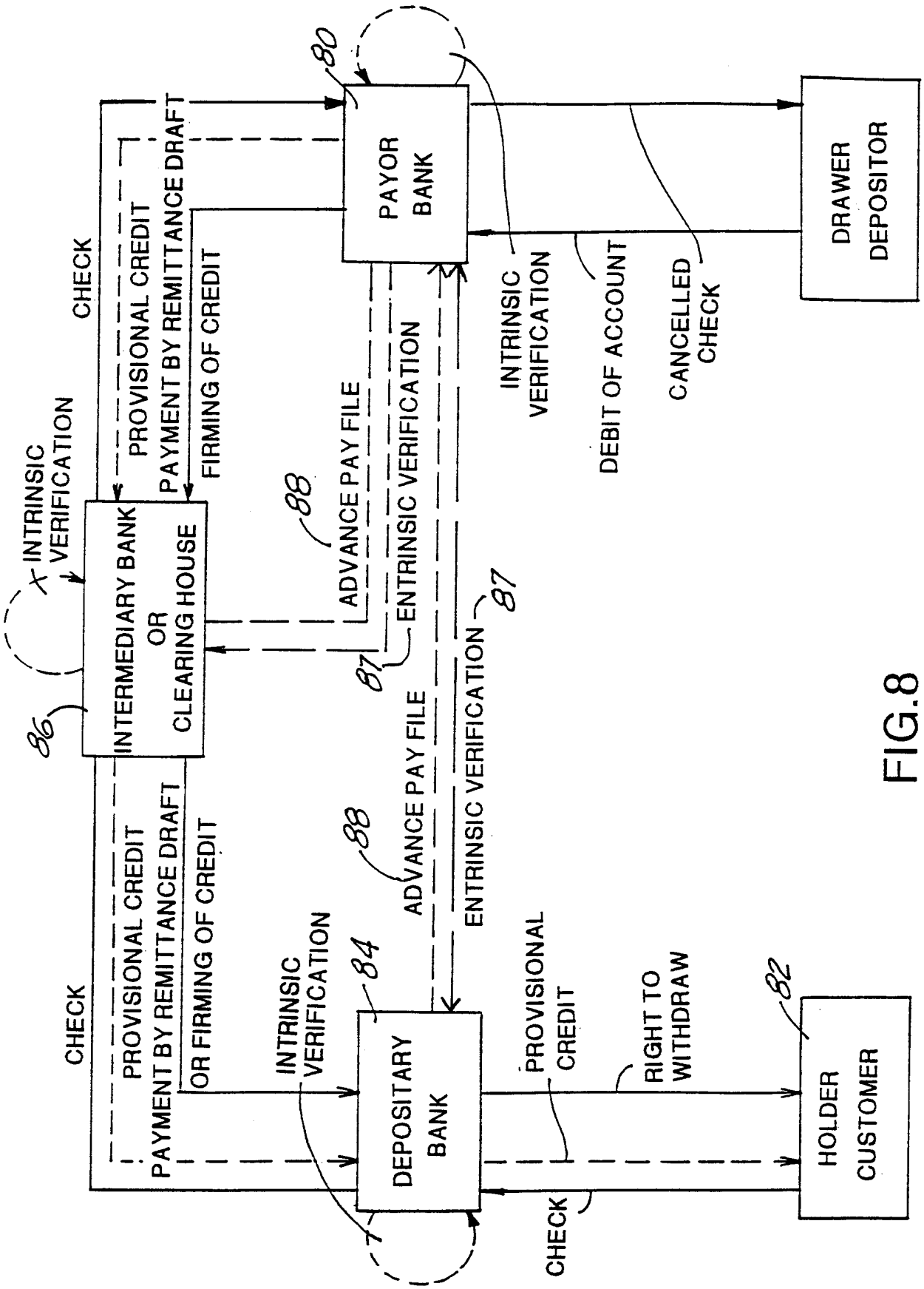

80
PAYOR BANK
DRAWER DEPOSITOR
CHECK
PROVISIONAL CREDIT
PAYMENT BY REMITTANCE DRAFT
FIRMING OF CREDIT
INTRINSIC VERIFICATION
DEBIT OF ACCOUNT
CANCELLED CHECK
88
ADVANCE PAY FILE
ENTRINSIC VERIFICATION
87
INTRINSIC VERIFICATION
86
INTERMEDIARY BANK OR CLEARING HOUSE
CHECK
PROVISIONAL CREDIT
PAYMENT BY REMITTANCE DRAFT
OR FIRMING OF CREDIT
88
ADVANCE PAY FILE
87
ENTRINSIC VERIFICATION
INTRINSIC VERIFICATION
84
DEPOSITARY BANK
PROVISIONAL CREDIT
RIGHT TO WITHDRAW
82
HOLDER CUSTOMER
CHECK

FIG.8

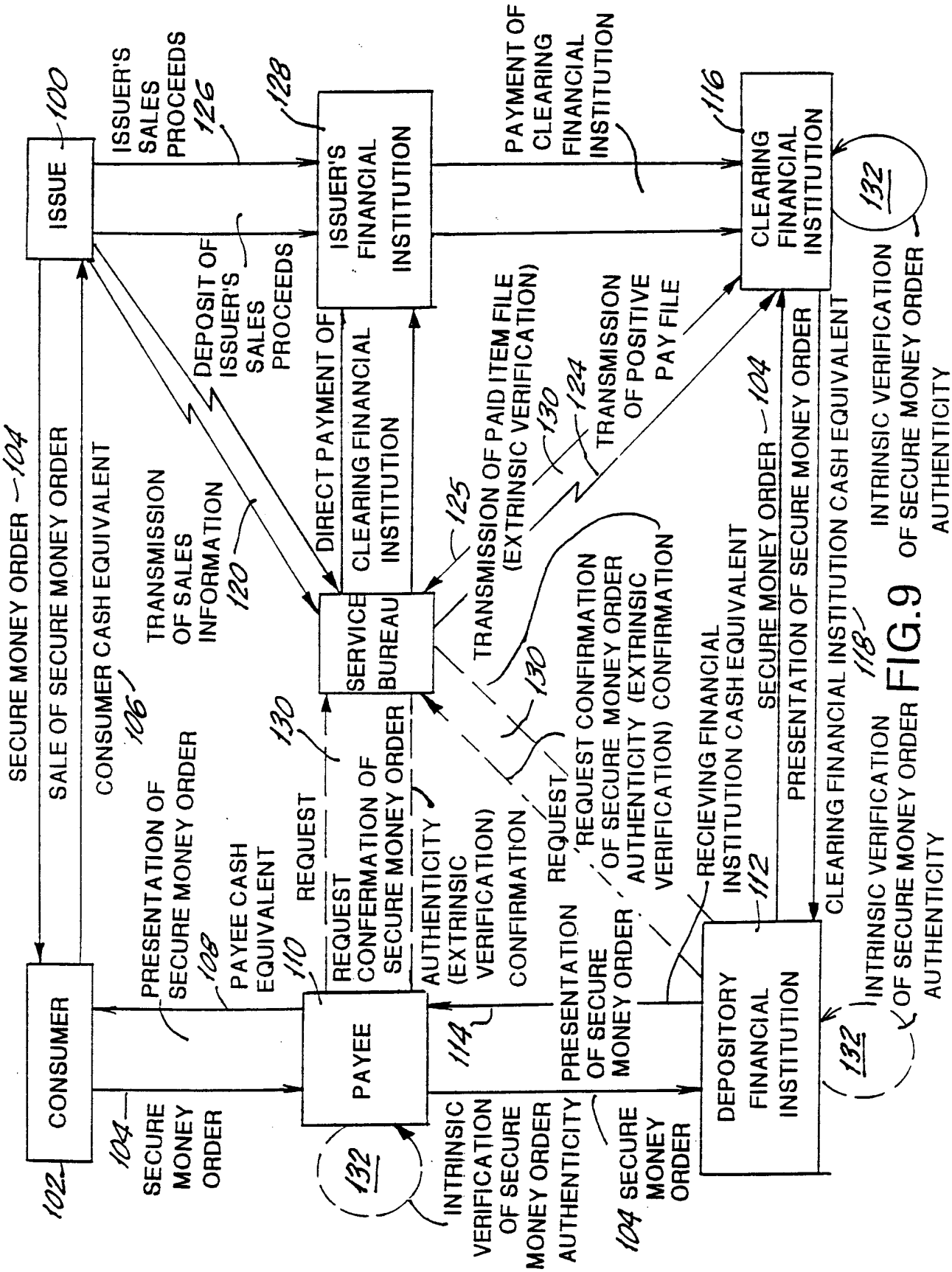

ISSUE
100
ISSUER'S SALES PROCEEDS
126
128
ISSUER'S FINANCIAL INSTITUTION
PAYMENT OF CLEARING FINANCIAL INSTITUTION
116
CLEARING FINANCIAL INSTITUTION
SECURE MONEY ORDER
104
SALE OF SECURE MONEY ORDER
CONSUMER CASH EQUIVALENT
106
DEPOSIT OF ISSUER'S SALES PROCEEDS
TRANSMISSION OF SALES INFORMATION
120
DIRECT PAYMENT OF CLEARING FINANCIAL INSTITUTION
SERVICE BUREAU
125
TRANSMISSION OF PAID ITEM FILE (EXTRINSIC VERIFICATION)
130
124
TRANSMISSION OF POSITIVE PAY FILE
CONSUMER
102
SECURE MONEY ORDER
104
PRESENTATION OF SECURE MONEY ORDER
108
PAYEE CASH EQUIVALENT
110
REQUEST
REQUEST CONFERMATION OF SECURE MONEY ORDER
130
AUTHENTICITY (EXTRINSIC VERIFICATION)
CONFIRMATION
REQUEST
REQUEST CONFIRMATION OF SECURE MONEY ORDER AUTHENTICITY (EXTRINSIC VERIFICATION) CONFIRMATION
PAYEE
114
PRESENTATION OF SECURE MONEY ORDER
104
SECURE MONEY ORDER
RECIEVING FINANCIAL INSTITUTION CASH EQUIVALENT
112
SECURE MONEY ORDER
104
PRESENTATION OF SECURE MONEY ORDER
118
CLEARING FINANCIAL INSTITUTION CASH EQUIVALENT
DEPOSITORY FINANCIAL INSTITUTION
132
INTRINSIC VERIFICATION OF SECURE MONEY ORDER AUTHENTICITY
132
INTRINSIC VERIFICATION OF SECURE MONEY ORDER AUTHENTICITY

FIG.9

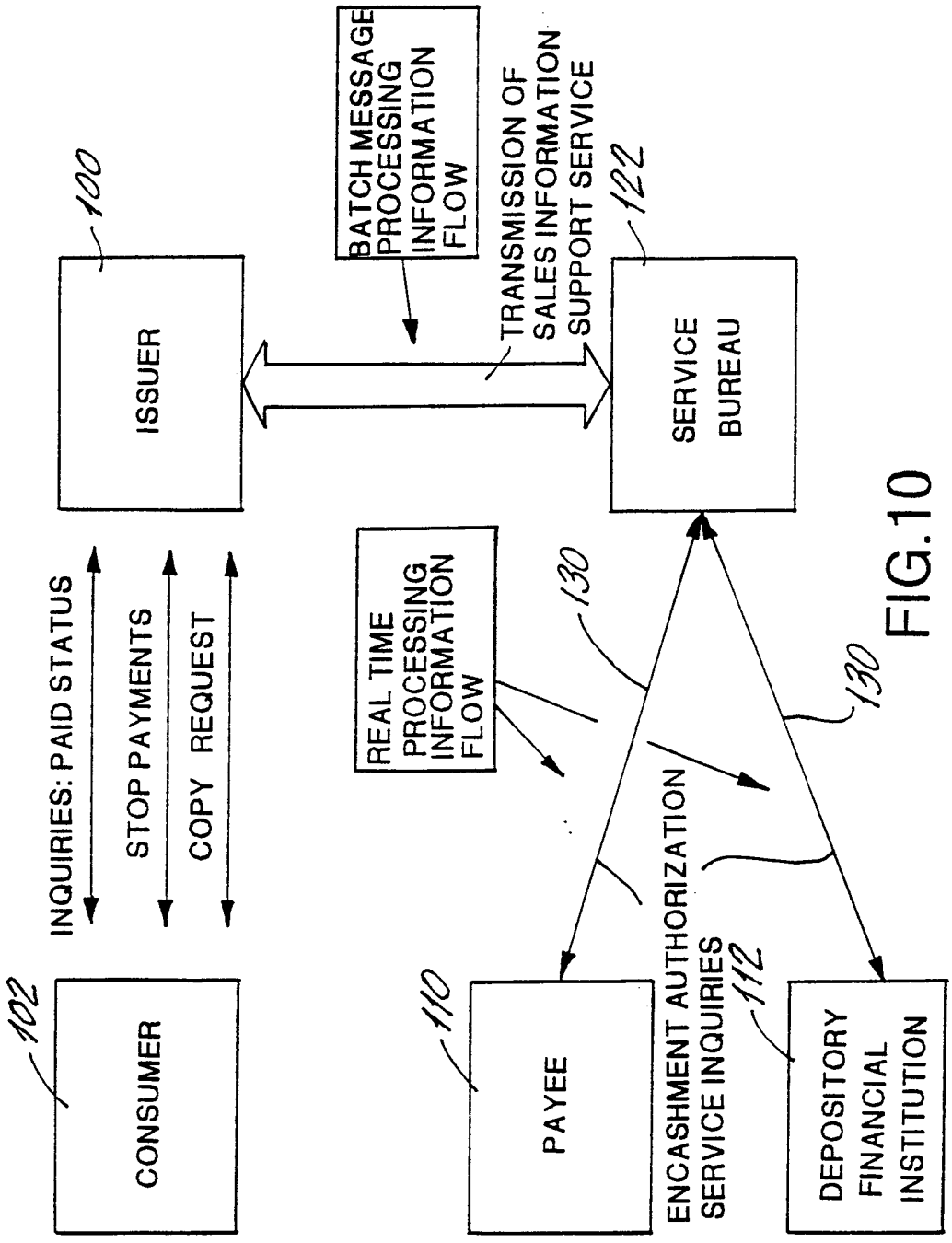

100
ISSUER
BATCH MESSAGE PROCESSING INFORMATION FLOW
TRANSMISSION OF SALES INFORMATION SUPPORT SERVICE
122
SERVICE BUREAU
INQUIRIES: PAID STATUS
STOP PAYMENTS
COPY REQUEST
REAL TIME PROCESSING INFORMATION FLOW
130
130
102
CONSUMER
110
PAYEE
ENCASHMENT AUTHORIZATION SERVICE INQUIRIES
112
DEPOSITORY FINANCIAL INSTITUTION

FIG.10

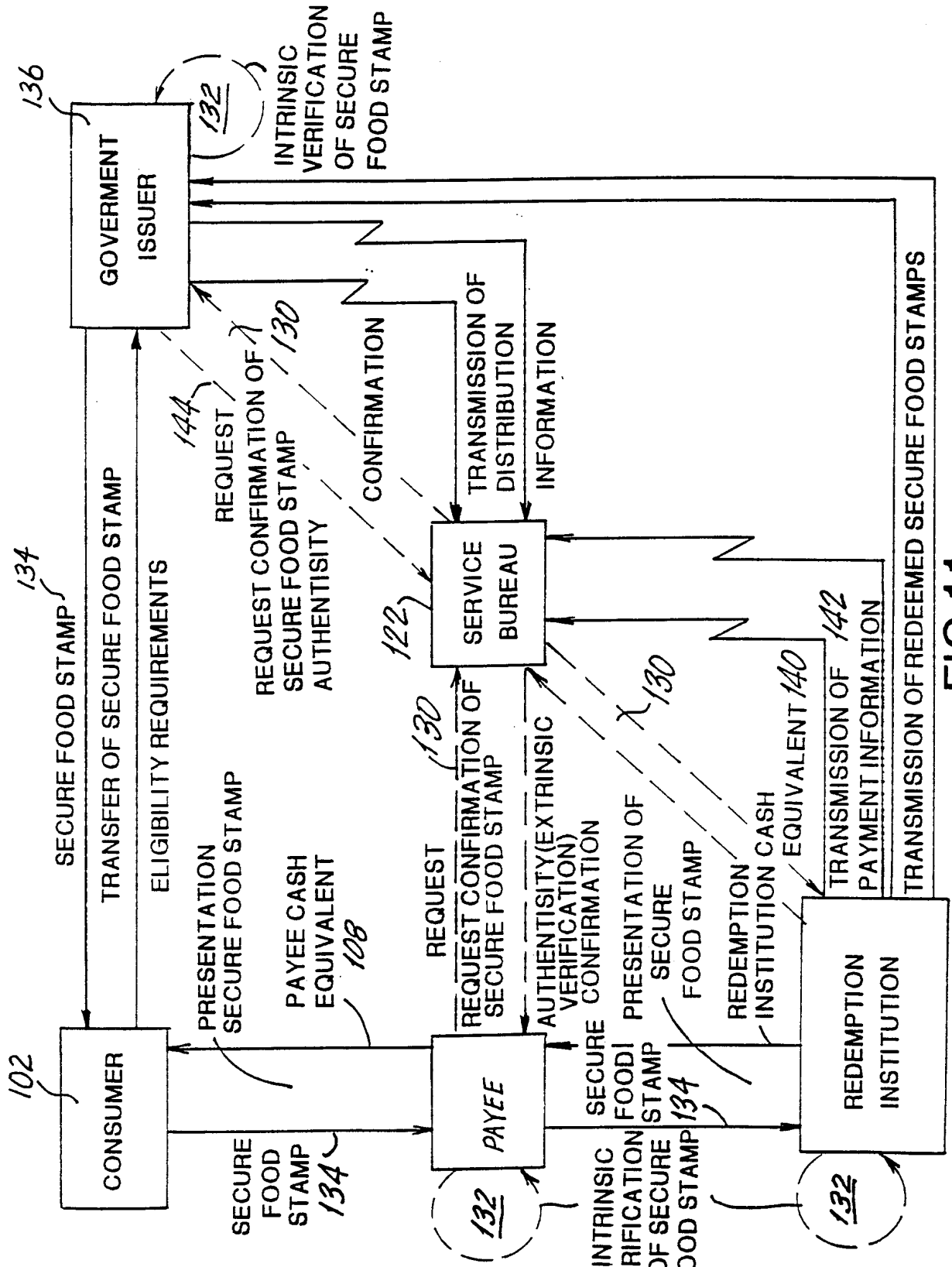

GOVERMENT ISSUER
136
132
INTRINSIC VERIFICATION OF SECURE FOOD STAMP
SECURE FOOD STAMP
134
TRANSFER OF SECURE FOOD STAMP
ELIGIBILITY REQUIREMENTS
REQUEST
144
REQUEST CONFIRMATION OF SECURE FOOD STAMP AUTHENTISITY
130
CONFIRMATION
TRANSMISSION OF DISTRIBUTION INFORMATION
SERVICE BUREAU
122
CONSUMER
102
PRESENTATION SECURE FOOD STAMP
PAYEE CASH EQUIVALENT
108
REQUEST
REQUEST CONFIRMATION OF SECURE FOOD STAMP
130
AUTHENTISITY(EXTRINSIC VERIFICATION)
SECURE CONFIRMATION
PRESENTATION OF SECURE FOOD STAMP
134
REDEMPTION INSTITUTION CASH EQUIVALENT
140
TRANSMISSION OF PAYMENT INFORMATION
142
TRANSMISSION OF REDEEMED SECURE FOOD STAMPS
PAYEE
REDEMPTION INSTITUTION
SECURE FOOD STAMP
134
INTRINSIC VERIFICATION OF SECURE FOOD STAMP
132
132

FIG.11

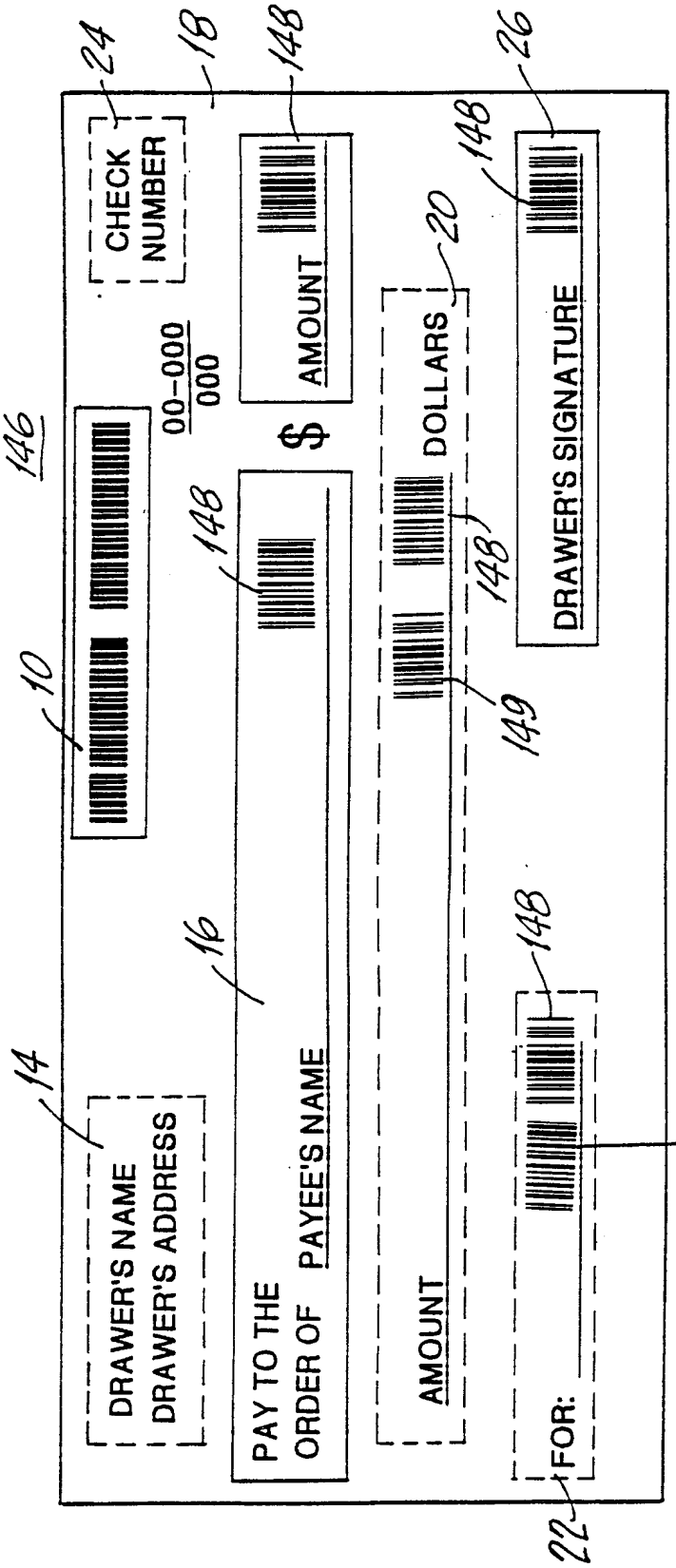

24
18
148
26
CHECK NUMBER
00-000/000
AMOUNT
$
146
148
148
DOLLARS
20
10
148
DRAWER'S SIGNATURE
149
16
PAY TO THE ORDER OF PAYEE'S NAME
14
DRAWER'S NAME
DRAWER'S ADDRESS
AMOUNT
148
FOR:
149
22

FIG.12

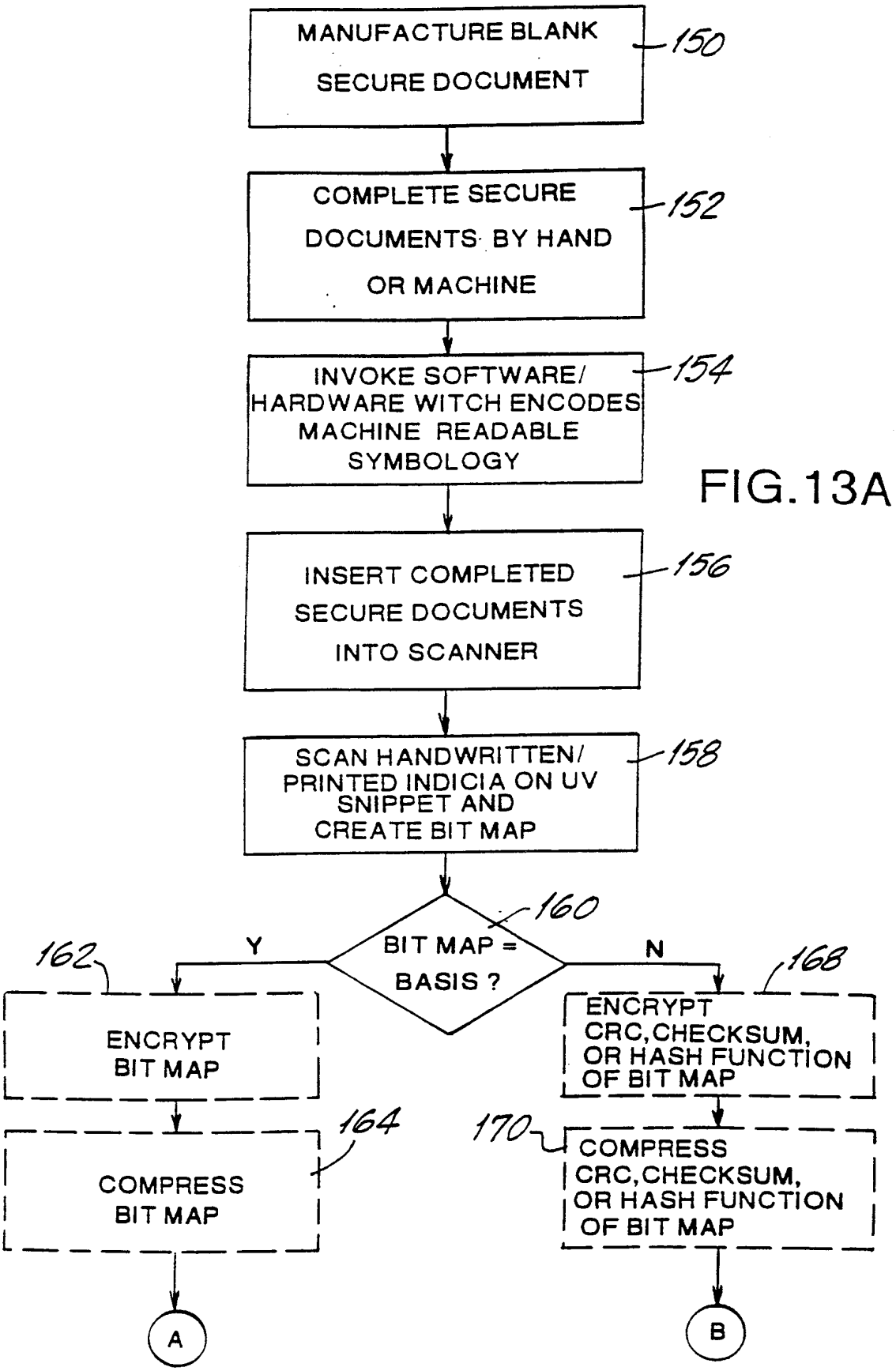

MANUFACTURE BLANK SECURE DOCUMENT
150
COMPLETE SECURE DOCUMENTS BY HAND OR MACHINE
152
INVOKE SOFTWARE/ HARDWARE WITCH ENCODES MACHINE READABLE SYMBOLOGY
154
INSERT COMPLETED SECURE DOCUMENTS INTO SCANNER
156
SCAN HANDWRITTEN/ PRINTED INDICIA ON UV SNIPPET AND CREATE BIT MAP
158
BIT MAP = BASIS ?
160
Y
N
162
ENCRYPT BIT MAP
164
COMPRESS BIT MAP
A
168
ENCRYPT CRC, CHECKSUM, OR HASH FUNCTION OF BIT MAP
170
COMPRESS CRC, CHECKSUM, OR HASH FUNCTION OF BIT MAP
B

FIG.13A

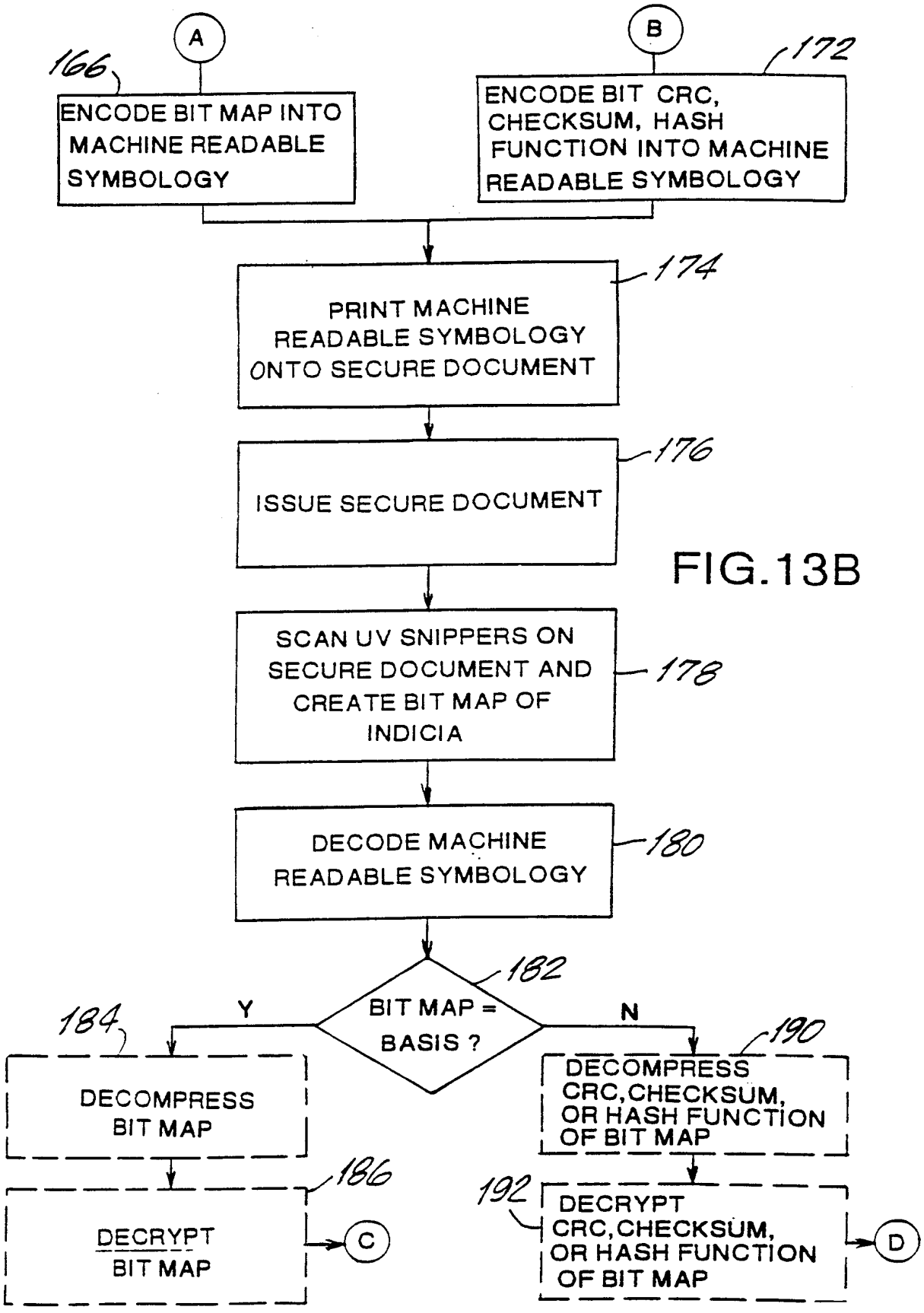

A
166
ENCODE BIT MAP INTO MACHINE READABLE SYMBOLOGY
B
172
ENCODE BIT CRC, CHECKSUM, HASH FUNCTION INTO MACHINE READABLE SYMBOLOGY
174
PRINT MACHINE READABLE SYMBOLOGY ONTO SECURE DOCUMENT
176
ISSUE SECURE DOCUMENT
SCAN UV SNIPPERS ON SECURE DOCUMENT AND CREATE BIT MAP OF INDICIA
178
DECODE MACHINE READABLE SYMBOLOGY
180
182
BIT MAP = BASIS ?
Y
N
184
DECOMPRESS BIT MAP
186
DECRYPT BIT MAP
C
190
DECOMPRESS CRC, CHECKSUM, OR HASH FUNCTION OF BIT MAP
192
DECRYPT CRC, CHECKSUM, OR HASH FUNCTION OF BIT MAP
D

FIG.13B

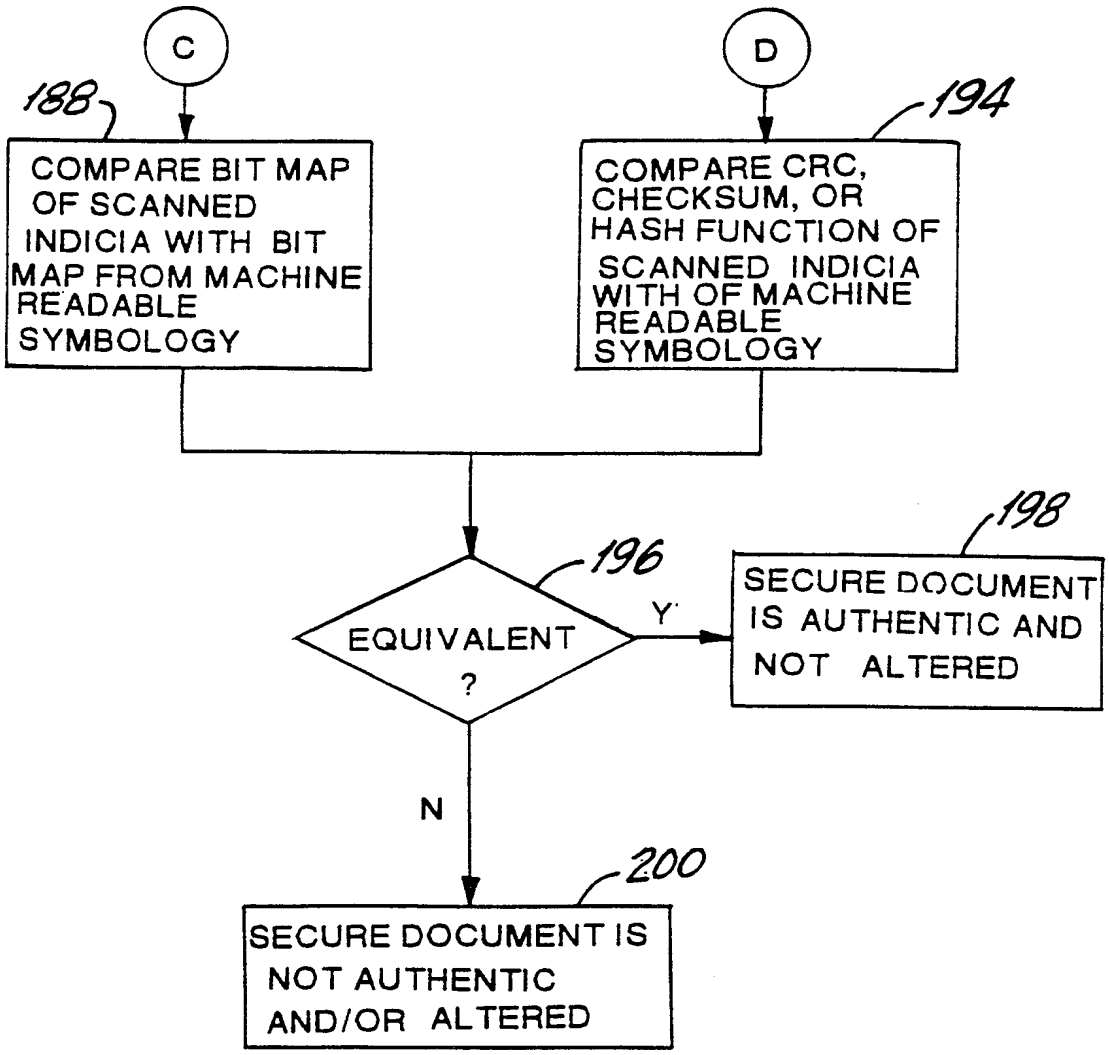

C
D
188
194
COMPARE BIT MAP OF SCANNED INDICIA WITH BIT MAP FROM MACHINE READABLE SYMBOLOGY
COMPARE CRC, CHECKSUM, OR HASH FUNCTION OF SCANNED INDICIA WITH OF MACHINE READABLE SYMBOLOGY
196
198
EQUIVALENT ?
Y
SECURE DOCUMENT IS AUTHENTIC AND NOT ALTERED
N
200
SECURE DOCUMENT IS NOT AUTHENTIC AND/OR ALTERED

FIG.13C

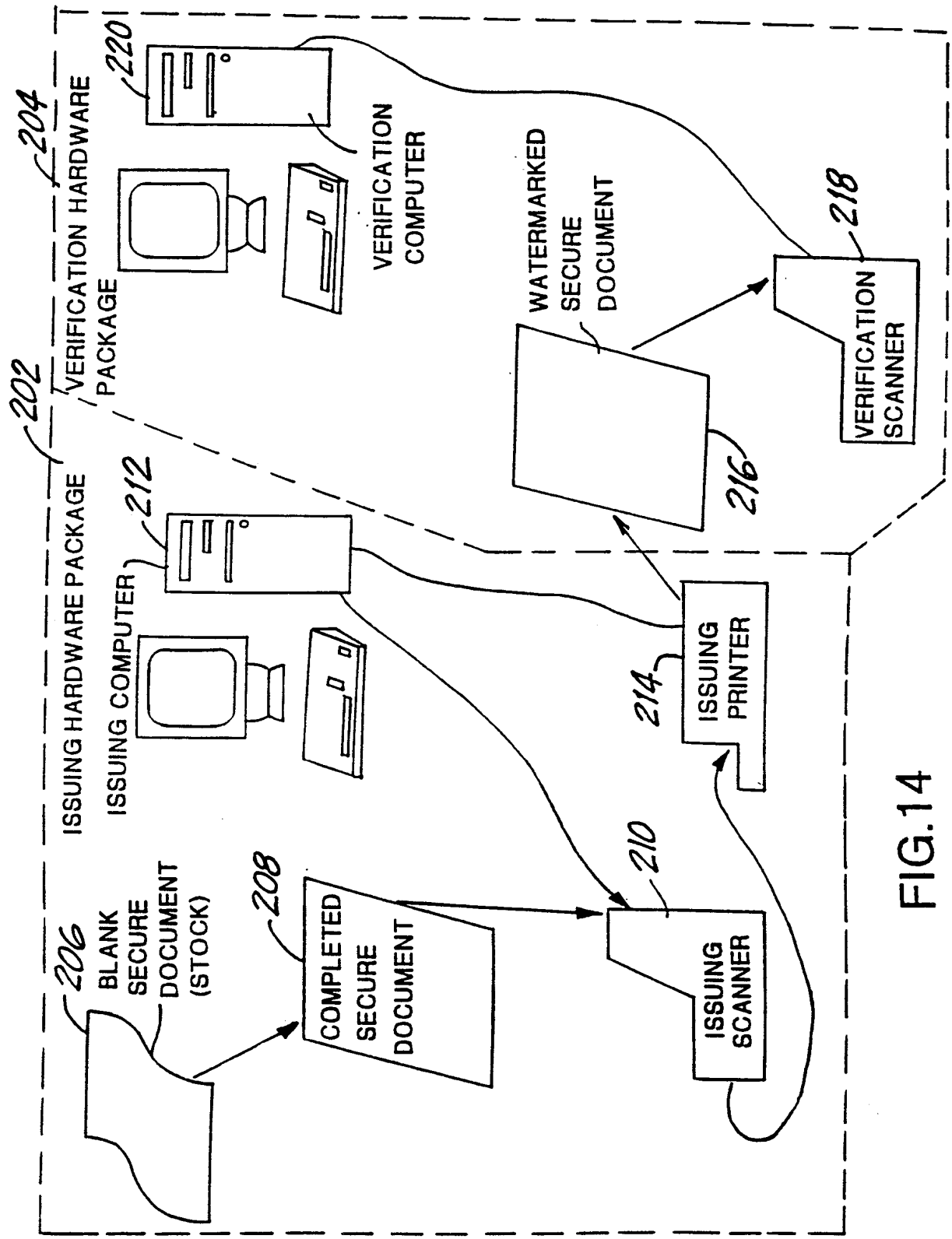

202
ISSUING HARDWARE PACKAGE
204
VERIFICATION HARDWARE PACKAGE
206
BLANK SECURE DOCUMENT (STOCK)
208
COMPLETED SECURE DOCUMENT
210
ISSUING SCANNER
212
ISSUING COMPUTER
214
ISSUING PRINTER
216
WATERMARKED SECURE DOCUMENT
218
VERIFICATION SCANNER
220
VERIFICATION COMPUTER

FIG.14

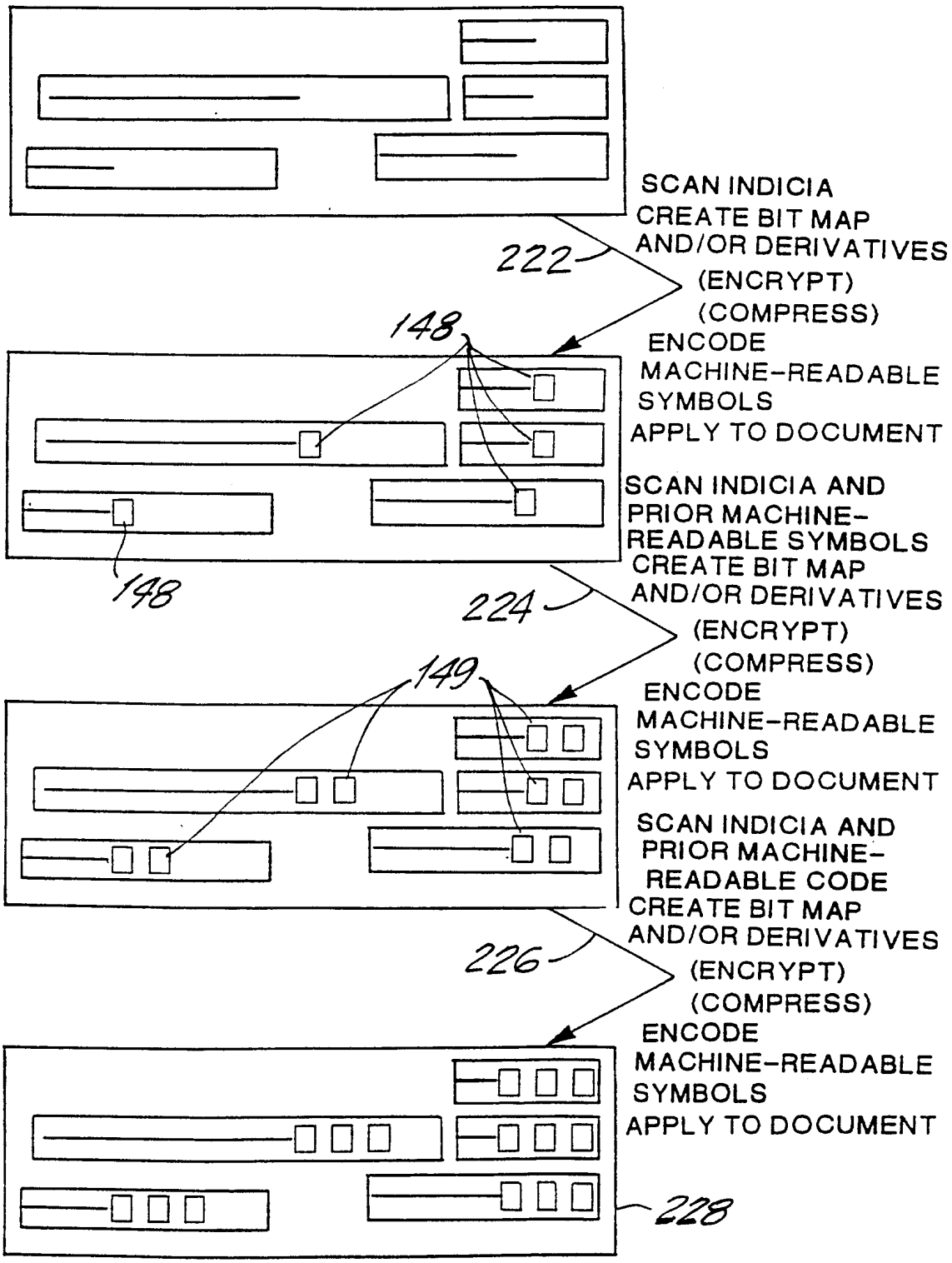

SCAN INDICIA
CREATE BIT MAP
AND/OR DERIVATIVES
(ENCRYPT)
(COMPRESS)
222
148
ENCODE
MACHINE-READABLE
SYMBOLS
APPLY TO DOCUMENT
SCAN INDICIA AND
PRIOR MACHINE-
READABLE SYMBOLS
CREATE BIT MAP
AND/OR DERIVATIVES
148
224
(ENCRYPT)
(COMPRESS)
149
ENCODE
MACHINE-READABLE
SYMBOLS
APPLY TO DOCUMENT
SCAN INDICIA AND
PRIOR MACHINE-
READABLE CODE
CREATE BIT MAP
AND/OR DERIVATIVES
226
(ENCRYPT)
(COMPRESS)
ENCODE
MACHINE-READABLE
SYMBOLS
APPLY TO DOCUMENT
228

FIG.15

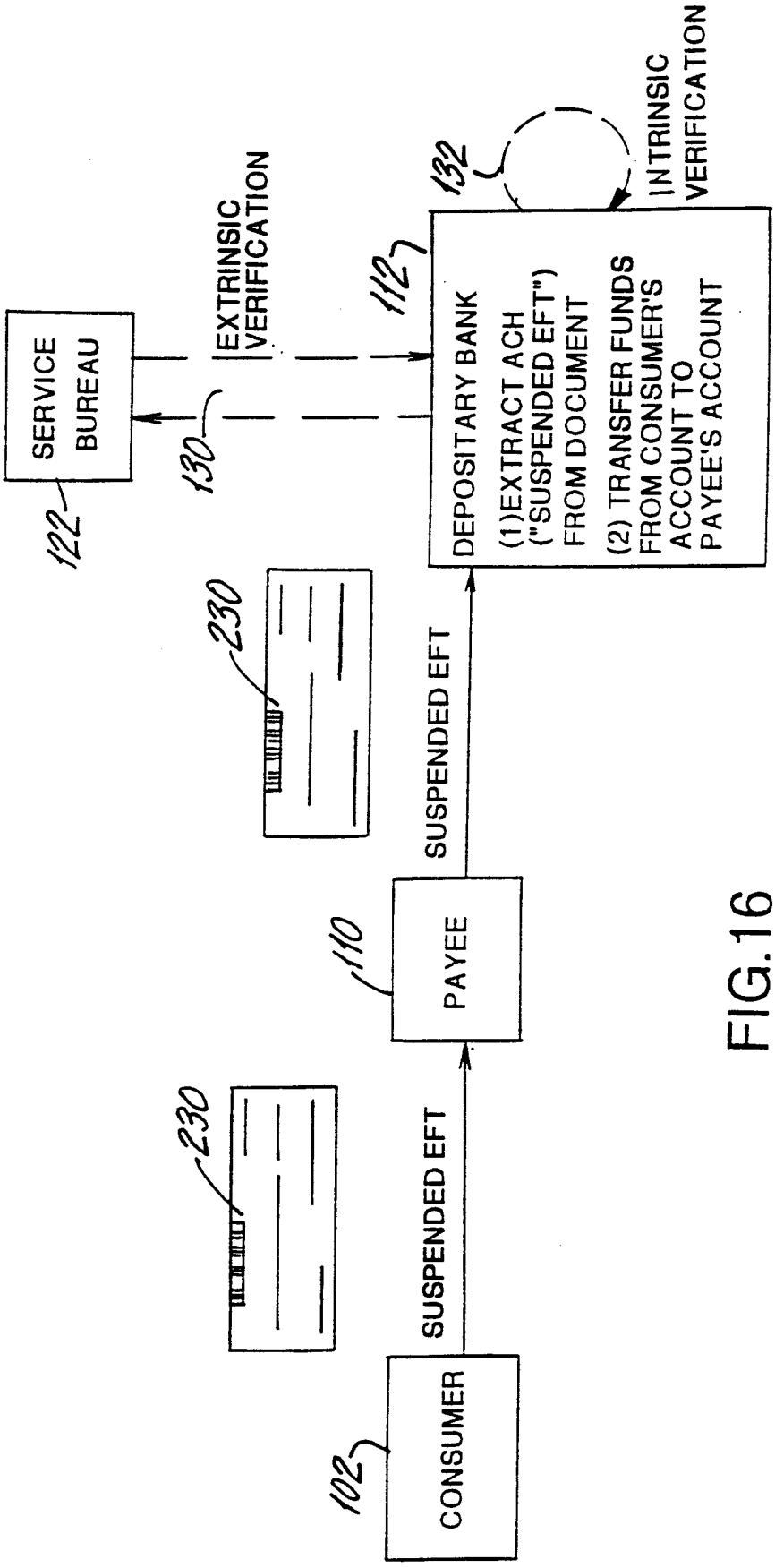

CONSUMER
102
SUSPENDED EFT
230
PAYEE
110
SUSPENDED EFT
230
DEPOSITARY BANK
(1)EXTRACT ACH ("SUSPENDED EFT") FROM DOCUMENT
(2) TRANSFER FUNDS FROM CONSUMER'S ACCOUNT TO PAYEE'S ACCOUNT
112
INTRINSIC VERIFICATION
132
EXTRINSIC VERIFICATION
130
SERVICE BUREAU
122

FIG.16

CONSUMER
CASHIER
MERCHANT CENTRAL DATABASE
SERVICE BUREAU
1. SELECT BLANK SECURE MONEY ORDER FROM DISPLAY AREA
2. TRANSFER TO CASHIER
3. SCAN SECURE MONEY ORDER
4. COMPLETE AMOUNT OF SECURE MONEY ORDER
5. TRANSMIT ISSUANCE INFORMATION
6. RECORD AND PROCESS ISSUANCE INFORMATION
7. TRANSMIT ISSUANCE INFORMATION
8. RECORD AND PROCESS ISSUANCE INFORMATION
9. TRANSMIT AUTHENTICATION INFORMATION
10. RECORD AND PROCESS AUTHENTICATION INFORMATION
11. TRANSMIT AUTHENTICATION INFORMATION
12. ACTIVATE SECURE MONEY ORDER
13. TRANSFER RECEIPT AND SECURE MONEY ORDER (IF NOT AN ELECTRONIC FUND TRANSFER) TO CONSUMER

FIG.17

CONSUMER
CASHIER
MERCHANT CENTRAL DATABASE
SERVICE BUREAU
1. SELECT SECURE GIFT CERTIFICATE FROM DISPLAY AREA
2. TRANSFER TO CASHIER
3. SCAN SECURE GIFT CERTIFICATE
4. COMPLETE AMOUNT OF SECURE GIFT CERTIFICATE
5. TRANSMIT ISSUANCE INFORMATION
6. RECORD AND PROCESS ISSUANCE INFORMATION
7. TRANSMIT ISSUANCE INFORMATION
8. RECORD AND PROCESS ISSUANCE INFORMATION
9. TRANSMIT AUTHENTICATION INFORMATION
10. RECORD AND PROCESS AUTHENTICATION INFORMATION
11. TRANSMIT AUTHENTICATION INFORMATION
12. ACTIVATE SECURE GIFT CERTIFICATE
13. TRANSFER RECEIPT AND SECURE GIFT CERTIFICATE

FIG.18

FIRST NATIONAL BANK
MasterCard

0000 0000 0000 0000

EXPIRATION 2/99

United States Postal Money Order 00-000/000

□□□□□□ □□□ □□□□ *□□*□□

PAY TO	CHECKWRITER $$
ADDRESS	FROM
	ADDRESS
COD No. OR USED FOR	

FIG.19

PUB-NO: WO009913391A2
DOCUMENT-IDENTIFIER: WO 9913391 A2
TITLE: IMPROVED SECURE DOCUMENTS
PUBN-DATE: March 18, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
CHRISTIANSEN, ROBERT	N/A
DURST, ROBERT T JR	N/A
GREENE, JONATHAN D	N/A
KEEPPER, LESTER H JR	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEOMEDIA TECH INC	US

APPL-NO: US09818571
APPL-DATE: September 4, 1998

PRIORITY-DATA: US05815397P (September 8, 1997) , US06503397P (November 10, 1997)

INT-CL (IPC): G06F00/

EUR-CL (EPC): G07F007/08 , G07D007/00

ABSTRACT:

CHG DATE=19990905 STATUS=O>A method of generating and

verifying secure documents (12) wherein the secure document (12) is printed with machine-readable symbols (28) representing physical parameters of the secure document prior to application of hand or machine-printed indicia, human and/or machine-printed indicia appearing thereon, biometrics (finger and voice prints), and transaction history. In another embodiment, a two-stage imaging or watermark process captures an image of indicia within an area defined by a ultraviolet coating (30), prepares a bit map thereof and encodes the bit map and/or a derivative thereof in machine-readable symbols that are then printed on the secure document (12). Intrinsic verification of the secure document (12) is accomplished by comparing actual physical measurements and scannings of the secure document with the data content of the machine-readable symbols appearing on the secure document. Extrinsic verification of the secure document is accomplished by comparing information content resident in local and/or remote databases concerning the secure document or its transfer with the data content of the machine-readable symbols appearing on the secure document.